THIS PUBLICATION CONSISTS OF TWO PARTS:

A) REPORT

B) PRESENTATION

Information Security Legislation

Comments on circulating drafts

Jennifer Bayuk
Chair, SIA Information Security Subcommittee

Information Security Technology Legislation as seen by a financial industry information security officer.....

1. Introduction

Concerns about identity theft have motivated a plethora of legislation directed at safeguarding information. Information security professionals are often requested to comment on these proposals. Rather than comment on any one proposal, this paper will review the objectives of any such legislation and survey the issues to be considered in meeting those objectives.

Information security is a safeguard against information theft. However, there is no universally accepted definition of *information theft*. Information must be shared in order for it to be processed. *Information communication* is the act of transferring data between individuals. A definition of information theft must cover cases where people legitimately have access to the information they have stolen and also cases where they do not. An example of a case where initial access is legitimate is the case of the Help Desk clerk. That person must have access to names and account numbers in order to perform a job function. However, the personal information shared with the help desk clerk is not intended to be a transfer of possession. An example where initial access is not legitimate is the commonly cited example of an Internet hacker stealing credit card databases.

In this paper, the term *information theft* will refer to the transfer of information to an individual that is not specifically authorized to possess that information via processes adopted by the information owner. This definition presupposes a clear *information owner* and *readily identifiable*, *transparent processes* by which information is processed in conformance with the wishes of the information owner. Any audit of compliance with existing legislation (e.g. GLBA, Sarbanes Oxley) must assume that these terms can be clarified. However, there is presently a gap between generally accepted information systems control guidelines and auditable standards which to support this clarification. This gap has led legislatures to lose focus on the information dissemination issue and instead propose technology measures to be used to control information processing. This paper proposes clarification that would make legislation concerning information theft a straightforward prospect. It also discusses why various technology-based proposals for closing the gap are off target.

2. Landscape

Figure 1 provides an illustration of the opportunities for data theft in electronic form. In the first column, labeled, “Criminals target,” the “Security Assessment Confidence Level,” is meant to indicate, for each type of electronic storage, how likely data is to be targeted by criminals. These assessments accurately reflect the general opinion of qualified information security professionals. The second column is a factual statement on the typical level of Internet-accessibility associated with the given type of data storage mechanism.

It is generally thought safe to assume that criminal threat likelihoods increase as data becomes more Internet-accessible. However, Figure 1 illustrates that simply the fact that a data is accessible from the Internet does not determine the likelihood that data will be a criminal target. It

Figure 1:

Security Assessment Confidence Level (High,Medium, Low,None):

Data can be stolen:	Criminals target:	Internet Accessible:
In transit	L	H
From media	L	N
From hand-helds	L	L
From desktops	H	H
From Servers		
via financial industry applications	H	H
via retail applications	H	H
via financial industry oper systems	H	L
via retail operating systems	H	M

varies with the format of the data, because the data format can sometimes determine whether the criminal act is likely to succeed.

For example, Internet network transmissions are of course readily accessible via the Internet. However, most criminals do not have direct access to network transmission devices outside of their own neighborhood. The level of technical sophistication it takes to overcome this obstacle makes network transmission in general a low probability target. The data that is in transit on the Internet is of course Internet-accessible. However, it only appears on the path between two systems at the time they are communicating. To rely on transit interception as a method of stealing identity data, a criminal has to be in the right place at the right time. He or she would also have to reconstruct the data from the transmission stream. Although it is possible to do this with unlimited time and computing resources, targeting data in transit is not the easiest way to steal identity data.

In the judgement of most information systems security professionals, criminals are much more likely to directly target identity data in situations where the data is static than where it is time-dependent. Yet the existence of static data is also not the sole defining factor in whether criminals will target it. Were this type of accessibility the only factor in gauging the likelihood of data left, there would be far more attention to identity information on storage media, where storage media usually refers to backup tapes. However, tapes and other such media are routinely kept in offsite storage facilities that are not connected to the Internet. So the likelihood that they are Internet-

accessible is none. The format of data on these tapes usually makes it difficult to read with inexpensive off-the-shelf or free software. Criminals are also seen as more likely to steal data where they can easily access the software used to read it than where they cannot. In addition, to find the one tape that contains current identity information in a storage warehouse would require considerable insider knowledge of both the computing environment in which the tape was made and the computing environment of the storage service provider. Moreover, a criminal would also need physical access to the storage facility to steal the storage media. Therefore, the probability that criminals will target storage media looking for identity information is normally assessed as low.

Similarly, hand-helds are not normally targets because of the physical access and readability requirements. This of course applies to hand-helds only to the extent that they are stand-alone and not configured to be directly accessed via wireless networks. Where they are network-connected, there is no logical difference between the hand-held and a desktop. However, two practical differences make the hand-held less of a target. One is that large quantities of personal identity information is not normally stored on hand-helds. Names and phone numbers aside, it is atypical for businesses to implement processes where by customer account numbers combined with personal information are stored on hand-helds. The other difference is that hand-helds are not consistently on the network, in which case the ability to steal data from them becomes time-dependent.

Desktops, by contrast, meet both aspects of the high risk profile. They are normally connected to the Internet and there are plenty of programs available with which to read desktop data. Companies that provide data over the Internet must also provide software with which consumers read data, and this makes company servers high criminal targets as well. The terms by which to distinguish the operation of data-serving software from the operation of the machine upon which it resides are *application* and *operating system*, respectively. The combined term *application server* often refers to a machine dedicated to the processing of application data such as a Retail Shopping Cart application. Application servers require data-reading methods to be readily available in order to be of service to the average consumer. This makes them more of a criminal target. Operating systems are also high criminal targets even though they are less likely to be Internet-accessible than application systems. This is because they are likely to have access to data from multiple types of applications within a company.

The “Server” rows in Figure 1 list servers in the retail and financial industries separately to illustrate that criminals target not only financial industry applications and servers, but also retail industry applications and servers. Personal identity information is equally likely to be available in both types of applications. Operating system servers in the both industries are usually surrounded by firewalls that prevent direct Internet accessibility. It is widely recognized among information security professionals that the financial industry in general has better controls than most other industries, retail included, so financial industry servers are listed as less Internet-accessible than retail ones. Nevertheless, as operating systems in both of these industries are known to contain significant quantities of identity data, both are likely to be targeted by identity thieves.

Figure 1 frames the information theft problem as primarily one of protecting data on desktops, applications, and servers from being criminal targets. The problem solution must also include

protective measures against the time and place network transmission attack. But in the face of exponentially growing numbers of Internet attacks on personal identity, electronic protection mechanisms on storage media or hand-held devices should be a secondary consideration.

3. Draft Legislative Technology Measures

Of the legislation that is focused on technology, by far the most common type of information security legislation calls for encryption or biometrics to prevent theft of data.

Encryption

Encryption is a reliably effective method of preventing data theft in cases where the algorithm is very strong, the key is unguessable, or the key changes with a frequency that renders decryption processes too expensive and/or time-consuming to derive much benefit from even a successful theft attempt. Encryption is an effective method of protecting data in network transmissions because the algorithms used for transmission are usually reasonably strong and they usually use hard-to-guess keys that change frequently. Encryption can also be reliably effective for preventing theft of data from media and hand-helds. The wide variety of strong algorithms available to encrypt data on these devices make the algorithm itself hard to guess, and, to decrypt the data, one must also guess the key. The requirements for an exploit of encrypted data on media and hand-helds include knowing the algorithm, physical access to the device, and correctly guessing the key. The combination renders the overall probably of exploit fairly low.

However, the probability of an exploit rises as the physical barrier and key change frequency decrease. Theft of encrypted data sitting on a desktop connected to the Internet does not require the serendipity of physical access or the cracking of time-sensitive keys. Thus, it is more probable assume an exploit of encrypted data on desktops than an exploit of encrypted data on network, media, or hand-helds. But given that a desktop will usually allow theft of only one individual's data, the likelihood that desktop encryption would deter theft of desktop data is still substantial.

Data encrypted on servers, by contrast, is more likely to be targeted. Like desktops, servers may be connected to the Internet, and if they store data encrypted, it is likely to be unlocked with a static key. Servers are likely to store identity data of many people rather than that of only a single individual. When an Internet user accesses their own personal data on a web page, they are accessing a server that is "serving" their data. Operating systems on servers perform this function by "hosting" application software that makes data available via the Internet.

The application server versus operating system differentiation yields a slightly lower probability of theft for encrypted data from operating systems than from applications. Usually, applications will encrypt identity data for Internet network transmission. Yet the data must be decrypted on receipt in order to be useful. Hence, even if application servers did store data encrypted, the fact that the application functions by making data available for display and manipulation requires the server to have decryption algorithms and keys readily available or to distribute them to desktops.

The above discussion of encryption explains the ratings in the third column of Figure 2. The last three columns in Figure 2 compare the data storage types of Figure 1 with respect to the

judgement of an informed information security professional as to the likelihood of the data protection mechanism in the column heading to successfully prevent theft of information from that type of data storage. Encryption alone will reduce likelihood of theft in network

Figure 2:

Security Assessment Confidence Level (High,Medium, Low,None):

Data can be stolen:	Criminals target:	Internet Accessible:	Encryption alone can reduce theft likelihood:	Industry standard authentication alone can reduce theft likelihood:	Biometric authentication alone can reduce theft likelihood:
In transit	L	H	H	L	L
From media	L	N	H	L	L
From hand-helds	L	L	H	L	L
From desktops	H	H	M	L	L
From Servers					
via financial industry applications	H	H	N	M	M
via retail applications	H	H	N	M	M
via financial industry oper systems	H	L	L	H	H
via retail operating systems	H	M	L	H	H

transmission, media, and hand-helds. It is somewhat less likely to deter consumer desktop accessibility because consumers tend not to choose very hard keys with which to encrypt and most algorithms used for desktop encryption are readily available. Nevertheless, the existence of encryption on a desktop will reduce the probability that it will be targeted. Encryption is not at all likely to reduce theft of application data as thieves will use the same methods authorized users use to get to the data. It is somewhat more likely to protect operating system data. But because the data must be used by the business, the encryption algorithms and keys are still likely to be as accessible to a criminal as the encrypted data itself.

All this means that a data thief would not be likely to attack the stored encrypted data as a means of stealing information, but to try instead to impersonate an authorized system user. Different types of thefts via user impersonation, like different type of thefts via decryption attempts, have different probabilities of exploit. For example, a single desktop on the Internet may have a low probability of being penetrated for theft of identity data. If a user were to encrypt the disk as well, encryption may be a sufficient deterrent to send the criminal somewhere else. However, if key choices are left to end users, they are easy, and also often stashed in places where the user can easily find them. In which case, a computer hacker impersonating the user can guess or find them. This reduces the decryption attack to an attack on the user login.

Authentication

The tendency for hackers to pursue impersonation is most likely the motivation for draft legislation requiring biometrics to be used as a login mechanism. The formal information security term for a computer user that is logged in is "authenticated user." Authentication refers to the process by which a user is determined by an application or operating system to correspond to a given *identity.* The term for the user name, or login, that someone uses when accessing a computer is *identity.* A valid user name by itself *identifies* the user to the computer as a person that is allowed to have access. However, not until the user enters some information that corresponds to the user name and can be used to *validate* the identity is the person assumed by the data-serving application to be that user. The process of validating the user identity is called *authentication*. The most common form of authentication is a password.

Various proponents of other forms of authentication claim that hand-held devices that have passwords that change every few seconds, various forms of biometrics, and/or digital certificates provide authentication mechanisms superior to passwords and thus should replace passwords as authentication. A oft-repeated phrase in information security training is, "What you know, What you have, and What you are." What you know commonly refers to a password. What you have commonly refers to a digital certificate or a hand-held authentication device. What you are commonly refers to a biometric. The lesson assumes that this is a hierarchy. This training material encourages a student to memorize two assumptions:

- A password can be given away by two people knowing it, but something you have cannot easily be shared. A digital certificate cannot be memorized, and a hand-held token, if given away, disables the valid user.
- A valid and sufficiently complex biometric reading that matches a computer record of the same person's previous recorded valid and sufficiently complex biometric reading provides a high level of assurance that the person from whom the reading is taken is the same person from whom the matching reading was taken.

Unfortunately, neither of these assumptions as stated correspond to the reality implemented by today's information security technology offerings. Digital certificates can be stolen and copied. Hand-held are often lost and must be replaced. The inconvenience has led vendors to allow work-arounds such as "soft tokens" that allow the hand-held authentication algorithm to be imitated by a desktop computer. Biometric devices often break and sometimes are purposely programmed to take insufficiently complex readings due to performance considerations. Both technologies are subject to spoofing by technically sophisticated hackers. Biometrics often has false positive and false negative readings because the matching algorithms employed are often based on heuristics. Difficulties with both technologies have led many application support groups to operationalize "bypass" utilities that allow a help desk user to assist an end user in gaining access. A hacker attempting user impersonation is not likely to be deterred from the effort by not possessing a token or fingerprint.

Whichever method of authentication is used, it can accomplish only so much toward protection of data. The fourth column in Figure 2 is meant to demonstrate that authentication is only one component of protection against theft of identity data. Authentication is only a preventive access control when it is required for access. It is not a control against reading data on network

transmissions via shared cable networks. It provides no control against reading data directly off of physically stolen hard drives or media. Most importantly, impersonation is not the only recourse for hackers who attack desktops and servers. Features of desktop, application, and operating system software often provide data extraction mechanisms that do not require a user to login. Sometimes these features are intended by software vendors and knowingly coded by developers. Call these unauthenticated features. Sometimes they are intended by software vendors, but not intended by the information system owner. Call these unauthorized features. Sometimes they are unintended by either the software developer or the end user. Only in the third case are they formally classified as vulnerabilities.

Figure 2 rates operating systems with authentication at a higher security confidence level than applications with the same authentication because operating system software usually has a large community of users that routinely test security configuration. Applications, by contrast, are usually specific to one business, and there is a high level of inherent risk involved in designing custom Internet applications. Hence, only at the server operating system level is it widely recognized among security professionals that tightly integrated strong authentication provides an adequate level of control. The fifth column of Figure 2 is meant to illustrate that all technology that today allows users to bypass existing authentication mechanisms also apply to authentication mechanisms that utilize biometrics.

Financial applications generally also provide tight integration of access control with data serving software. However, access to data through applications is not controlled by the login processes that rely on authentication. Rather, they are controlled by application code that determines which data a user with a given identity is allowed to access. The login provides only the identity. The application then determines which data to serve to the user based on the identity. For example, if a user logs into a bank site and the bank determines that the user holds three accounts at that bank, the user will be able to use the application to access data of all three accounts. Banks manage the mapping of user identity to account data via a process called *authorization*. Authorization itself relies a form of data, the data that maps a user to the data he or she is entitled to access. The map itself is often referred to as an *entitlement*. Because authentication processes happen only on login, both unauthenticated features and vulnerabilities are often the result of poorly programmed authorizations and entitlements.

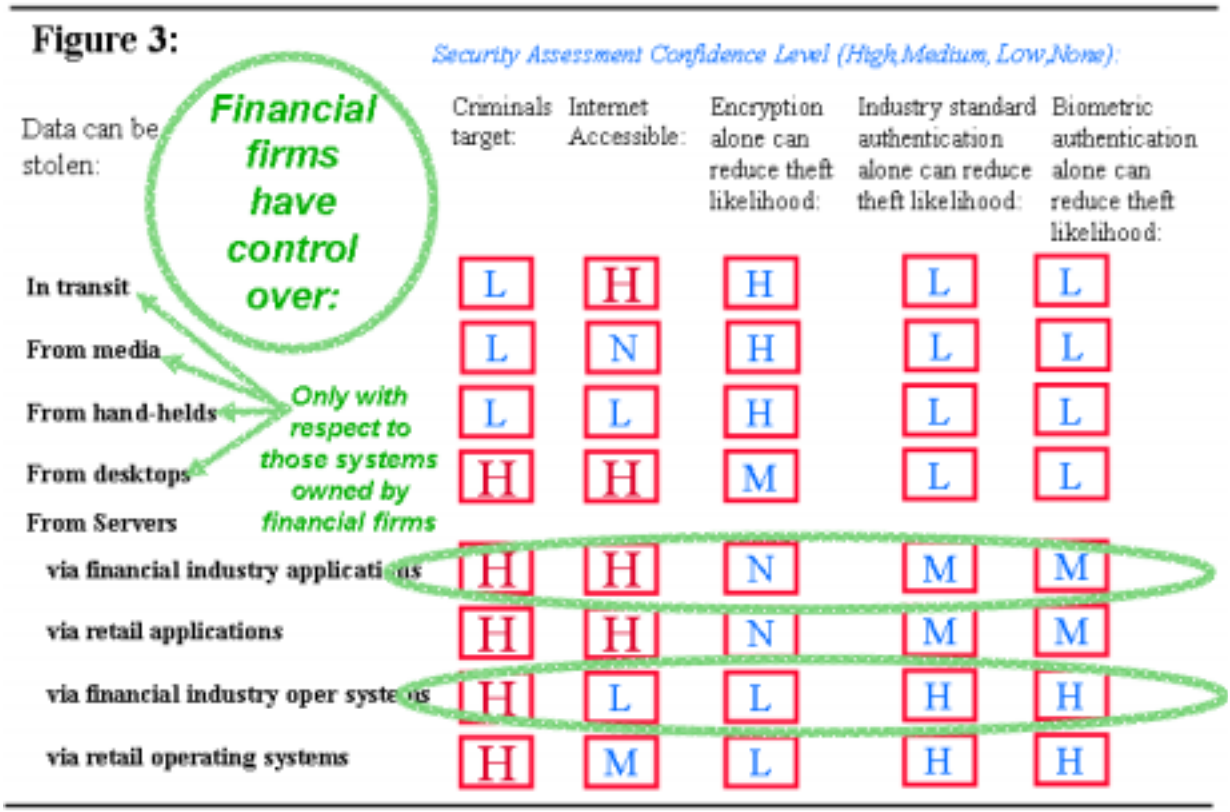
The reason why entitlement authorization is required over and above authentication is because of the way most application software works. Application software generally has access to a database that includes all user data, not just the data of the logged-in user. Applications must be programmed to check entitlements in order to decide which data to deliver to the user screen. A term for the process by which an authenticated user can request and receive data for which he or she has not been specifically entitled is called a *loophole*. Loopholes can be intentionally malicious vulnerabilities programmed into application code by rogue programmers or they can exist by accident. They can exist accidentally due to some unknown operating system or third party software functionality. They can exist accidentally due to vulnerabilities in operating system or third party software. Only in the last case can loopholes be closed by *patching,* another technology that sometimes catches the legislative eye. Loopholes can and often do exist due to simple errors in application programming that fail to restrict data access according to entitlements. In this case, they exist accidentally due to inadequate testing of security features.

Application software is usually so customized that no amount of security software or patching is likely to completely control the problem. In addition, programmers may not fully understand the real-world use of the application and may, as a result, omit critical security functionality.

The conclusion to be drawn from Figure 2 is that desktops and applications should not be assumed to require authentication to access data. These technologies rarely require authentication when first delivered by vendors. Information system owners must configure their systems to be secure. In fact, consumer desktops have so many unauthorized features designed to let advertisers and vendors read and manipulate home computers that even when consumers try to set their desktops to require authentication, they still have no control against malware and data theft. Sophisticated information technology departments will identify and disable unauthenticated and unauthorized features prior to storing data on operating systems. However, not all information technology departments are that sophisticated and not all software running on operating systems maintains the level of access control that an information technology group expects.

4. Financial Industry Concerns

Recent information security draft legislation has specified not only the type of security controls that should be in place, some versions also specify that the financial industry should implement those controls. Were the financial industry to be the only industry required to implement technology controls against theft of identity data, the level of risk areas addressed by the legislation would be that depicted in Figure 3. Figure 3 extends Figure 2 to show just what control



the financial industry is able to exercise over the data protection process. The uncircled high risk

areas would remain fertile ground for identity information theft. Were legislation with respect to information security to apply only to financial firms, it is unlikely to have any effect on the rate of identity theft.

The financial industry does not control security measures on desktops and hand-helds. The financial industry is one data steward, but it is not the only steward of identity data. Information stewards can only control data to the extent they can be said to possess it. Any requirements set by a bank or securities firm for securing consumer devices would be unenforceable. Similarly with applications and operating systems run by retailers. Contractual requirements and frequent audits can provide due diligence but can never provide assurance that security measures are faithfully adhered. An auditor is by necessity an independent outsider and will never be able to ascertain that all backdoors are plugged. In the areas where the financial industry does have control, it is not likely that encryption or biometrics legislation will lessen the overall likelihood of data theft. In the case of encryption, the likelihood that it will reduce risk is low. In the case of authentication, in the vast majority of financial institutions, reliable authentication is already being done. Criminals that bypass current authentication mechanisms will also be able to bypass biometric ones.

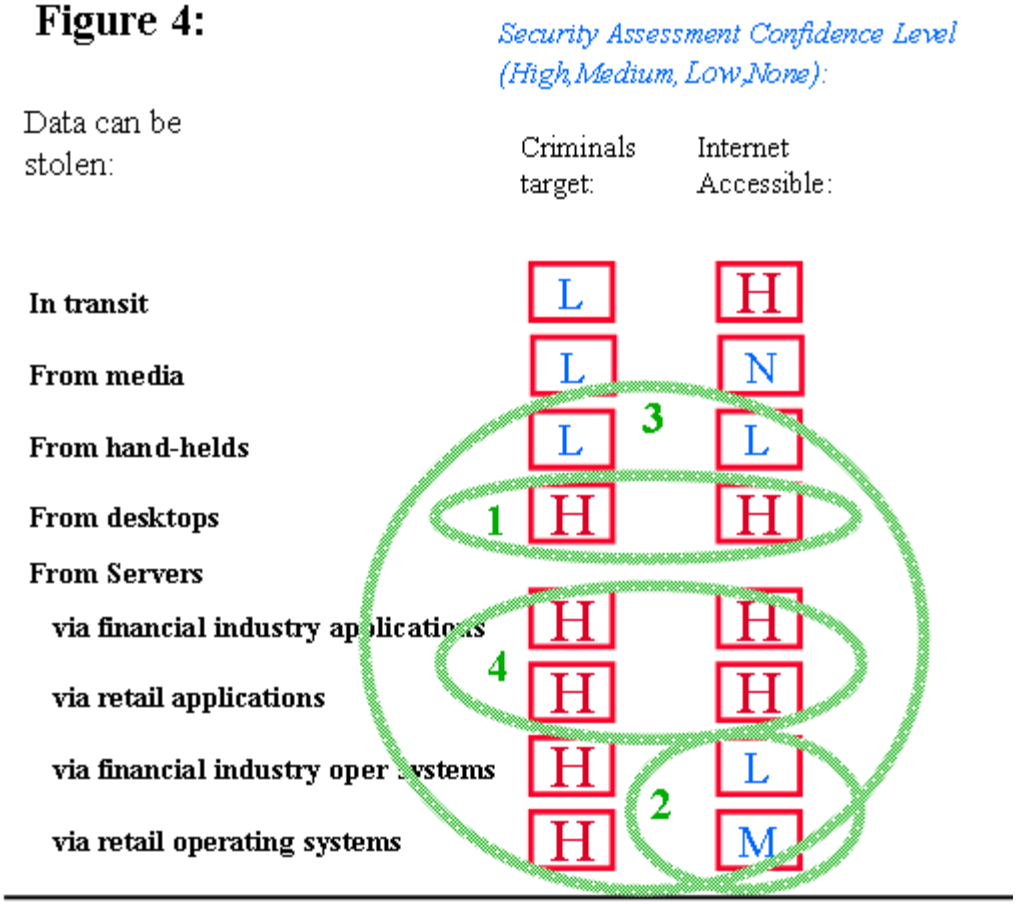
5. Gaps

Technology for protecting network transmissions from theft of identity data is not the subject of legislation. Nevertheless, nearly all financial and retail Internet services protect network transmission from theft using encryption. This came about because of the technology standards for browsers and web services. When the financial industry took to the Internet, it quickly recognized that the Internet Service Provider that carried its data out to the public was in the right place at the right time to view all the personal data. The easiest way to implement security for network transmission happened to be encryption. So encrypting data on the wire was one of the first generally accepted security controls. Because the financial industry educated their clients to see the lack of network encryption as a privacy concern, encryption of data in transit has become standard even in the retail industry. When auditors confirming compliance with GLBA look to verify that data is protected from theft during transmission, they view the implemented standard and no more legislation is needed. This is a exemplary case of industry creating its own standards without need of legislation.

Figure 4 shows where similar requirements exist at the desktop and server levels as these are also identified as either highly Internet-accessible or likely targets. But because concepts such as authentication, authorization, and entitlement are more custom and complex, these requirements have not yet been universally recognized as basic prerequisites for secure commerce. The numbers in the list of recommendations that follow correspond to the circled areas of concern.

1. It should be illegal to provision consumer desktops with software that can be exploited to run unauthorized programs.
2. Operating systems that serve personal data should never be Internet-accessible or publicly accessible (as may be in a non-Internet case making use of dial-up lines). Personal data should only be publicly accessible via applications that identify, authenticate, and specifically authorize end users via entitlements.

Figure 4:



3. Where an individual allows personal information processing by an information steward, the information steward should be required to have a well-defined and auditable process for authorizing access that allows no default access and identifies the necessity for providing access to authorized individuals.
4. All providers of applications that use personal information on the Internet should be required to focus on secure coding practices. Legislation should require due diligence of the Sarbanes Oxley variety to ensure management accountability.

Legislation targeted at preventing identify theft could also benefit from a basic clarification of terms. Most drafts are currently unclear on the issue of who owns identity information. Once information is passed from consumer to company, there seem to be two likely candidates for the designation of information owner with respect to identity information. The candidates are the person identified by the information and the organization that collected the information. Yet, in practical terms, only the person identified by the information can rightly hold any claim to its ongoing validity and only the organization that collected the information may be presumed to have any control over its dissemination. It would be helpful to end the debate over whether the information owner is the person identified by the information, and to always call others that possess an information steward. This way, information theft can still refer to the transfer of information to an individual that is not specifically authorized to possess that information via processes adopted by the information owner. The process adopted by the information owner is

that of sharing information with the information steward to facilitate some service that is readily identifiable by the owner. This is the core reasoning behind GLBA. The information steward must show that identity information is used only for the purpose under which it was shared, or must inform the information owner.

Looking at existing legislation in this light, any case of information being shared without express authorization of the owner is easily identified as information theft. GLBA is now interpreted to hold information stewards accountable if privacy is breached beyond reasonable interpretation of documented opt-out provisions. Information owners who have not opted out of information sharing processes have also not gotten full rights under GLBA if information shared with stewards is stolen, as (presumably) the case of information sharing via theft was not in the opt-out notification clause. Proposed guidelines to clarify the response program required by GLBA section 501(b) could ensure that this interpretation was made standard.

Where the theft of identity information would threaten compliance with GLBA, presumably there would be a decrease in consumer confidence in the corresponding information steward. Were the GLBA violation to weaken consumer confidence to the extent they took their transactions elsewhere, the impact could possibly impact the future outlook and thus the books and records of the firm. Were this to be the case for a public company, the company's information theft prevention program would become a critical assets and require management to attest to its effectiveness under Sarbanes Oxley. Even without the stigma of a GLBA violation as motivation, instances of theft of identity data could be legislatively ruled as materially impacting financial assets, Sarbanes Oxley section 404 concerning the effectiveness of the internal control structure could be standardly interpreted to include safeguards against theft of identity information. Private companies and not-for-profits are currently exempt from Sarbanes Oxley, but would have to be brought into the fold as well. In the financial industry, many of the systems that process consumer transaction are already covered under Sarbanes Oxley, so the formality of including data confidentiality requirements would be easily integrated into an already well-defined audit process.

Though of course not the focus of this analysis, but nevertheless worthy of mention, information communication with respect to personal information need not just refer to electronic media. Data can be spoken, written, or encoded in a variety of ways. Information security legislation concentrates on the act of transferring data via bit patterns on electronic media readable by computers. From the perspective of information security legislation, data in possession is assumed to be electronic; that is, in network transmissions, storage media such as CDs and backup tapes, hand-helds, desktops, and servers. Perhaps because it is well recognized that, in the course of doing business, data must be verbally communicated and shared among those who need it to perform business functions, current information security legislation drafts do not attempt to proscribe procedures and processes by which those who are easily able to memorize data should be prevented from verbally communicating it. Rather, legislation drafts are targeted at electronic data, proscribing procedures by which electronic data should be prevented from being electronically communicated. This leaves a wide area for information theft from stewardship processes that would not be covered by legislation which focuses purely on technology. Computer crime law is all about what you can do using electronic data. Internal control structures designed

to deter theft of identity data should also provide safeguards against verbal sharing of personal information and social engineering.

6. Summary

This paper is about risk/reward trade-offs and about the current practicality of proposed alternative technical information security controls. It is set against the landscape of threats to demonstrate that if currently available and practical measures were followed, the vast majority of easy targets would disappear. This conclusion does not presume that any one directly targeted individual could not fall victim to a determined identity thief with an unlimited budget. Rather, practical legislation aimed at combating identity theft should aim to make stealing identity information the game of highly-funded, highly-technical, highly-motivated cybercriminals and not a game that is within the ability of a rising population of low-budget cyber-cons. Were this type of legislation enacted, when the dust settles, relatively few identity thieves will remain active due to their insider connections or highly advanced skills. To detect and individually investigate them should become a manageable exercise.

What are we talking about?

Information Theft is not: **something that occurs when those who are authorized instead use information for a purpose that is itself not authorized, i.e. misuse by authorized individuals**

Information Theft is: **unauthorized access + misuse**

This definition presupposes a clear information owner and readily identifiable, transparent processes by which information is processed in conformance with the wishes of the information owner.

We are talking about data.

Data is not: information overheard in a cafeteria

Data is: information formatted electronically

The definition of information as data allows a fairly comprehensive enumeration of the types of places from which information may be stolen:

In transit
From media
From hand-helds
From consumer desktops
From servers

Which becomes the “Threat landscape”

Data can be
stolen:

In transit

From media

From hand-helds

From desktops

From Servers

- **via financial industry applications**
- **via retail applications**
- **via financial industry oper systems**
- **via retail operating systems**

Threat landscape

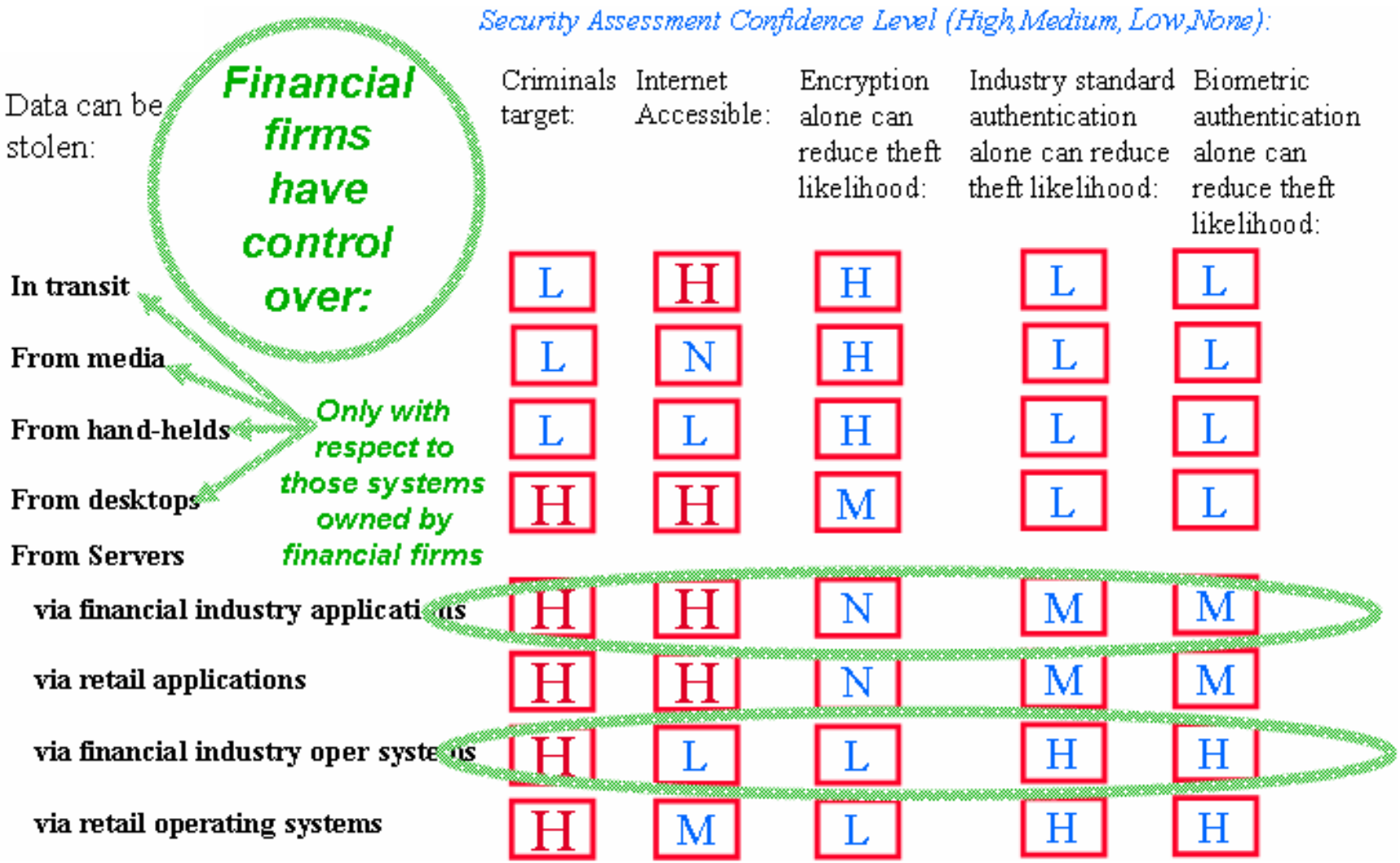
Data can be stolen:	*Security Assessment Confidence Level (High,Medium, Low,None):* Criminals target:	Internet Accessible:
In transit	L	H
From media	L	N
From hand-helds	L	L
From desktops	H	H
From Servers		
via financial industry applications	H	H
via retail applications	H	H
via financial industry oper systems	H	L
via retail operating systems	H	M

Corresponding Technology Safeguards

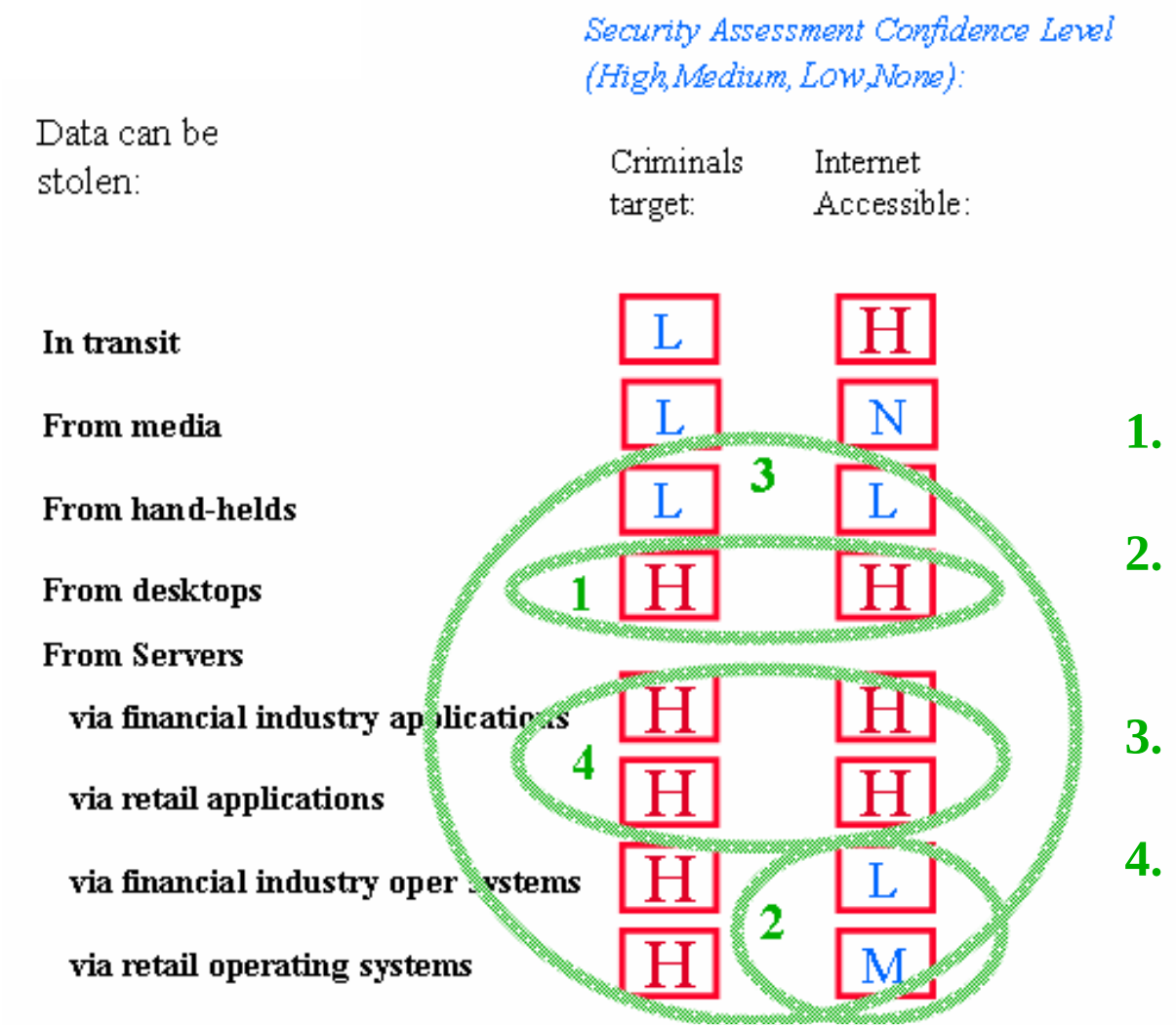
Security Assessment Confidence Level (High,Medium, Low,None):

Data can be stolen:	Criminals target:	Internet Accessible:	Encryption alone can reduce theft likelihood:	Industry standard authentication alone can reduce theft likelihood:	Biometric authentication alone can reduce theft likelihood:
In transit	L	H	H	L	L
From media	L	N	H	L	L
From hand-helds	L	L	H	L	L
From desktops	H	H	M	L	L
From Servers					
via financial industry applications	H	H	N	M	M
via retail applications	H	H	N	M	M
via financial industry oper systems	H	L	L	H	H
via retail operating systems	H	M	L	H	H

Individual Entity Control



Collective Exposure



1. **Exposed Desktops**
2. **Exposed Operating Systems**
3. **Distributed accountability**
4. **Specious entitlements**

Security Assessment Confidence Level (High,Medium,Low,None):

Data can be stolen:	Criminals target:	Internet Accessible:
In transit	L	H
From media	L	N
From hand-helds	L	L
From consumer desktops	H	H
From Servers		
via financial industry applications	H	H
via retail applications	H	H
via financial industry oper systems	H	L
via retail operating systems	H	M

It should be illegal to provision consumer desktops with software that can be exploited to run unauthorized programs.

Security Assessment Confidence Level (High,Medium,Low,None):

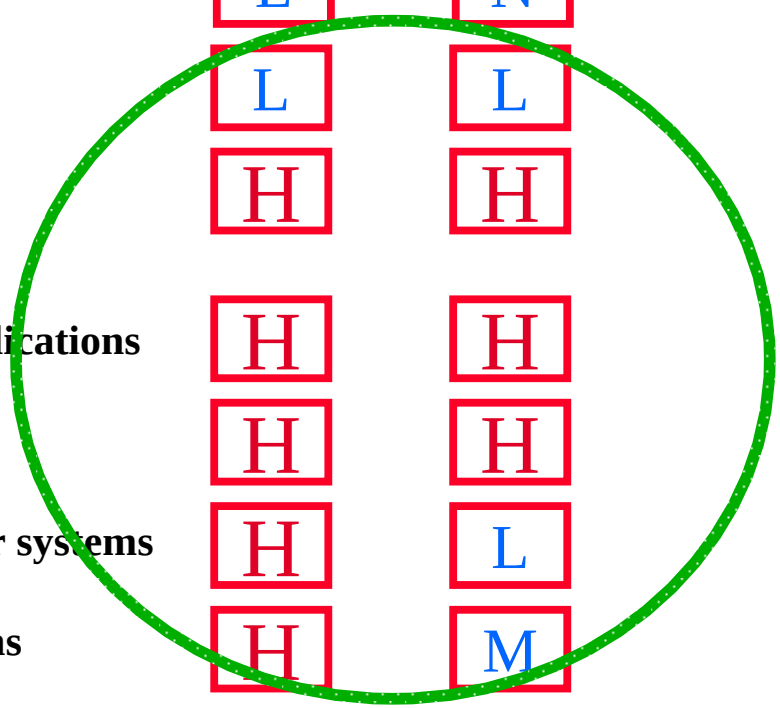
Data can be stolen:	Criminals target:	Internet Accessible:
In transit	L	H
From media	L	N
From hand-helds	L	L
From consumer desktops	H	H
From Servers		
via financial industry applications	H	H
via retail applications	H	H
via financial industry oper systems	H	L
via retail operating systems	H	M

Operating systems that serve personal data should never be Internet-accessible or publicly accessible (as may be in a non-Internet case making use of dial-up lines). Personal data should only be publicly accessible via applications that identify, authenticate, and specifically authorize end users via entitlements.

Security Assessment Confidence Level (High,Medium,Low,None):

Data can be stolen:

	Criminals target:	Internet Accessible:
In transit	L	H
From media	L	N
From hand-helds	L	L
From consumer desktops	H	H
From Servers		
via financial industry applications	H	H
via retail applications	H	H
via financial industry oper systems	H	L
via retail operating systems	H	M



Where an individual allows personal information processing by an information steward, the information steward could be required to have a well-defined and auditable process for authorizing access that allows no default access and identifies the necessity for providing access to authorized individuals.

Security Assessment Confidence Level (High,Medium,Low,None):

Data can be stolen:	Criminals target:	Internet Accessible:
In transit	L	H
From media	L	N
From hand-helds	L	L
From consumer desktops	H	H
From Servers		
via financial industry applications	H	H
via retail applications	H	H
via financial industry oper systems	H	L
via retail operating systems	H	M

All providers of applications that use personal information on the Internet should be required to focus on secure coding practices. Legislation could require due diligence of the Sarbanes Oxley variety to ensure management accountability.

Legislation

should be focused on:	**information handling process and management controls**
should not be focused on:	**technology**

This leaves the bar raised on the information steward.

Lack of technology will not be an excuse.

Purchase of “approved” technology will not absolve.