Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Business Justification for Data Security

It bears mention that, for reasons we ll explain in the following sections, we consider it impossible to rely completely on quantitative justiﬁcations, but we will show you how to combine quantitative and qualitative factors to make informed risk management decisions. We won t discuss speciﬁc technologies except as examples, but will instead focus on business aspects you can use in your discussions with management. Also, this isn t a generic model to justify any security spending instead...

Copyright SANS Institute
Author Retains Full Rights

AD

The Business Justification for Data Security

Version 1.0
Released: January 26, 2009

The SANS Institute http://sans.org

Securosis, L.L.C. http://securosis.com

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog but has been enhanced, reviewed by SANS, and professionally edited.

This report is licensed by McAfee Inc. and released in cooperation with the SANS Institute.

Special thanks to Chris Pepper for editing and content support.

Licensed by McAfee

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

http://www.mcafee.com

Copyright

This report is licensed under the Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 license.

http://creativecommons.org/licenses/by-nc-nd/3.0/us/

Table of Contents

Introduction 5

How security perceptions influence investment 5

Competing priorities: infrastructure and assets 5

Building business justifications 6

Data Loss Models 7

Understanding the value of data 7

Why there is no ROI for data security 7

The complexities of information valuation 9

Information Valuation Model 11

Valuation examples 12

Estimating Risk 14

Measuring and understanding the risks to information 14

Combining quantitative and qualitative risk estimates 14

Common data security risks 15

Potential Losses 19

Understanding Potential Losses 19

Quantified vs. Qualified Losses 19

Potential Loss Categories 20

Additional Positive Benefits 22

Cost savings and other positive benefits 22

Business Justification 25

Building the business justification 25

Step 3: Determine the potential risk reduction capability of the investment 26

Conclusion 29

Data Security Business Justification Worksheet 30

Step 3: Determine the potential risk reduction capability of the investment 32

Step 6: Business Justification Summary 36

About 37

About the Authors 37

About Securosis 37

About the SANS Institute 38

Introduction

How security perceptions influence investment

In the information security world we face two major types of threats: "noisy" threats which directly interfere with our ability to do business and "quiet" threats which cause real damage, but don't necessarily prevent people from doing their jobs. Noisy threats such as viruses, worms, and spam; attack both networks and systems, and clearly disrupt productivity and business operations. With highly visible (and often very annoying) attacks, it's easy to justify investments to curb their impact. When the CFO see hundreds of spam messages in his inbox, he's very likely to fund an anti-spam solution.

Quiet threats, such as data theft, are far more insidious — they can go undetected for years. When they are eventually discovered, you may not be able to calculate the material damage the breach has caused. It's much harder to get the CEO to sign off on a hundred-thousand-dollar investment when you can't directly demonstrate a corresponding drop in profit or an asset loss. In many cases, such as the theft of a credit card, it's someone else who suffers the loss. That's why security investments for quiet threats are often forced upon us by regulation or contractual obligation, rather than being voluntary. The lack of perceived threat undermines our recognition of data security, and thus our ability to address it.

Competing priorities: infrastructure and assets

When we review security markets, it's clear products that protect against noisy threats receive far more security dollars than those which address quiet threats. Security spending today is focused on the 'perimeter' — that imaginary boundary that separates users and systems inside the company from everyone else. It's not that we've failed at perimeter security, or the investments were not justified, but systems and data usage have changed. We've made far more of our information accessible from common web browsers, while increasing remote access and relying more on distributed services. In a parallel evolution, our risks have changed, with attackers realizing it is both easier and more profitable to target our data. The deficiency lies in our distribution of security resources. In a sense, we are victims of our own success — now that the organizationally simple protections (such as firewalls) are well understood and broadly implemented, the battle has shifted to more subtle and involved problems.

Thus we're caught in a paradox. The threats against our perimeter security are still very real, but newer threats against information assets require much different security controls. We are often trapped in budget cycles where we continue to renew our existing security even if it isn't the most effective way to address current problems. It's far easier to get approval for a renewed maintenance agreement or upgrade than a new product. We also have substantial investments of time, training, and experience in managing older threats. We better understand the risks, management costs, and justifications. And let's be honest — it's always easier to fall back upon what you know, as opposed to what you need to learn.

Old threats also have a frustrating tendency to never fade away; even today we still see 10-year-old viruses and worms floating around the Internet. Thus we can't simply throw away our old infrastructure to focus on new threats, but we do need to recognize that the old infrastructure is not designed to deal with new challenges, and that our spending calculations are often woefully out of date. Quiet threats to data only see equal levels of investment after suffering a major (typically public) incident, or when we are forced by industry or government mandates. Thus we've spent far more on securing our networks and systems than securing the information assets that really power our business. Noisy threats used to be our biggest problem, but now we need to shift focus.

Building business justifications

We need to acknowledge that threats have changed, from noisy to quiet, from the edge of the organization to the center. We also need to understand that attackers' motivations have changed — web site defacement isn't the goal; fraud and data theft are. Denial of Service, worms, viruses, and spam are still issues; but these noisy threats are more important as vectors for data theft rather than end goals. This isn't about lost productivity or minor embarrassment, but very real risks to the functioning of the business. The question becomes: How can you assess the risks and adjust spending to focus on the primary threats to the business?

There are many proposed methods to show the benefits of spending on security, treating data security as a type of investment, but when attempting to justify spending in specific areas, most of these approaches simply don't work. Some models attempt to measure what can't be accurately measured, and collapse under their own cumbersome processes. Others rely upon purely qualitative reasoning, producing wildly inaccurate results. Most of the models are composed of illogical variations on proven economic formulae, which were designed to gauge efficiency or return on investment. In the case of security, which is an investment that produces neither revenue nor fully quantifiable results, this is asking for failure.

In this report we will focus on the business side of data security (also known as information-centric security) as we build a justification model to help you determine where, and how much, to invest in protecting your information assets. We'll start this report by reviewing why some common approaches fail, discussing their weaknesses, and highlighting common pitfalls to avoid. We then proceed to discuss how to measure the value of information, estimate potential losses from breaches, and gauge the associated risks that cause that loss. From there we will build our recommended model, which combines different assessment and justification techniques, and demonstrates additional value to the organization. No single model can reflect all aspects of all organizations, and we expect you to pick and choose what works best in your own situation.

It bears mention that, for reasons we'll explain in the following sections, we consider it impossible to rely completely on quantitative justifications, but we will show you how to combine quantitative and qualitative factors to make informed risk management decisions. We won't discuss specific technologies except as examples, but will instead focus on business aspects you can use in your discussions with management. Also, this isn't a generic model to justify any security spending — instead we'll focus specifically on information valuation and data security. All subsequent reviews of information valuation, risk and loss assessment, and positive benefits such as reduced TCO or audit costs come from this data-centric analysis. Our goal is to give you the tools you need to evaluate your situation and determine if the risks you face warrant spending on security.

Data Loss Models

Understanding the value of data

Security is a tool for risk management — its purpose is to allow organizations to take the greatest amount of risk they are comfortable with, in the safest way possible. By definition, risk management is about limiting loss, or the potential for loss. But it's impossible to understand loss if you don't have a handle on the value of what you could lose. In this section we'll dig into the value of information, and in the process show why you can't always assign a specific monetary value, but you can get a handle on its importance to your organization. As a byproduct, we'll show why models that depend on full quantification of information value are doomed to failure.

We start with a method to quantify and/or qualify the value of data, and then show how security protects that value — which isn't easy because value changes under different business contexts. We can calculate the value of information based upon what it could be sold for, as an enabler for certain business functions, as a competitive advantage in the marketplace, or as a combination of factors. And just to be clear on what we are talking about, we define *information* as *data with value*, which is one reason we prefer the term "information-centric security"" over "data security".

But first, let's highlight the failures of common models to show why a new approach is needed. Then we will introduce a model that quantifies the value of information where possible, qualifies other significant factors, and evaluates value by combining the two. We will provide specific examples of methods you can use and refine over time for your organization to better determine how much to invest in securing your data. Any such investment needs to rest on a good understanding of the assets to protect.

Why there is no ROI for data security

The first person to create a model for accurately calculating the monetary value of information should win the Nobel prize. We can't ignore the value of data, but we need to accept that we often cannot assign it an accurate dollar amount. This creates one of the more vexing business problems in information security. Security needs to undergo the same analysis and justification as any other IT or business project, but its fundamental function is limiting loss, and we can't accurately predict that loss since we don't know the value of what we're losing (and it changes all the time anyway). This isn't a radical new way of thinking, but the process itself is fairly difficult. To aggravate matters, the traditional models for justifying investment and spending simply don't apply. The statistics and metrics that seed these calculations are typically unavailable or unreliable, and the computations treat revenue and data loss as opposing values. Let's take a look at a couple models to show you what we mean:

Return On Investment (ROI): Repeat after me: There is no ROI for security spending. Anyone who tells you otherwise is wrong. Here's why: When applying ROI to data security, you attempt to quantify loss, and then substitute loss as revenue. Besides always producing a negative result, this model is a fundamentally flawed way to approach security spending for a couple of reasons. The first is that security precautions do not create a return or generate revenue, so by definition they cannot be used to calculate revenue. The equation is abused by substituting potential losses that cannot

be reasonably quantified for 'Return', in place of quantifiable financial gains. Further, expenses such as disaster recovery, legal costs, and regulatory costs can be estimated with a fair degree of accuracy; but indirect costs such as "loss of reputation", brand impairment, and loss of future business cannot be accurately be assigned dollar amounts. ROI is a well understood and commonly used financial equation, but it does not account for many of the relevant variables effecting revenue, or the non-linear costs for multi-incident breaches. The calculation is fine for controlled academic problems, but in context of losses due to data breach, it is a case of garbage in, garbage out.

Internal Rate of Return: Some use the Internal Rate of Return calculation to evaluate spending, but this not only suffers the error of substituting potential losses with a capital return, it compounds the problem by attempting to examine the efficiency of security investment against other forms of investment. Because the value of information is not fully quantifiable, and losses associated with different risk vectors vary, the results of the equation are, *at best*, a ballpark estimate. Right up there with trying to use Net Present Value, from a practical standpoint, this is just more garbage.

A couple additional models are more useful and more closely aligned to data security. One alternative to the ROI calculation is *Return On Security Investment, or ROSI*. It is essentially the ROI calculation, but substitutes returns with the risk exposure in dollars, which is multiplied by the percentage of the threat mitigated by the investment. Another alternative is the *Annualized Loss Expectancy (ALE)* calculation, which is the anticipated loss from a single event multiplied by the expected rate of occurrence. While both are more realistic approaches, they require an understanding of the cost and the pre/post frequencies of occurrence. Both approaches are again hampered by our inability to assign an exact monetary value to information, as when it comes to data security we lack tools to accurately measure either the frequency or cost of an event.

Let's take a closer look at ALE to demonstrate what we mean: consider costs associated with stolen laptops. An organization can hopefully track the number of lost laptops over the course of a year. They may even be able to track the number of lost laptops containing credit card information, giving a reasonably accurate rate of occurrence. The organization also knows that it costs them $3 per record to manage a breach notification, and the average lost laptop with credit card information contains 10,000 records. Using ALE they can accurately predict the annual cost resulting from lost laptops with credit card information, and compare that to the cost of encryption.

Of course, they can't measure their reputation or lost business costs, which for a single incident might be $0, but for multiple incidents might put them out of business as they lose all customer trust. Nor can they measure the costs associated with the loss of the intellectual property on the laptop; since there isn't any regulatory requirement for notification, statistical data regarding rates of occurrence and business impact are unavailable. Keep in mind we've chosen a situation that's easy to measure, as opposed to database breaches or information leaks which we can't even measure without implementing data security protections in the first place.

In practice, ALE as a comprehensive risk model becomes a meaningless equation as you end up multiplying an estimate by a guess and ignoring unknowns. Estimating rate of occurrence and what percentage of threat has been mitigated requires information that is simply not available. As we like to say, a guess multiplied by a guess is a wild-assed guess. Aspects of it may be useful, but we can't rely on it alone. That's why we combine quantitative and qualitative factors to make an overall assessment.

There is one additional factor that should be mentioned in regard to costs associated with lost & stolen information: Quiet security threats don't target the network or the users, they target data. A breach, data theft, or fraud is not always evident; and the direct risk of fraud may be borne by others. For example, a burglary results in items missing that would be discovered by the owners, while with data theft the original information remains intact and the owner may never know a copy has been taken. Further, the fraud itself may not be perpetrated against the company, as when stolen credit card

data is used to purchase goods from another merchant. Over and above the rate of occurrence, the monetary loss associated is a guess at best — even if you are aware of the occurrences. To hammer this point home, here are three real-world examples:

- It's well known that many popular songs, albums, and films appear on peer-to-peer file sharing sites before they are even released to the market. On the surface it seems reasonable that the music companies could calculate the volume of illegal file sharing of their content, multiply that by retail costs of the items, and determine losses. But other studies claim that the very content that's most frequently illegally traded is also the most frequently bought legally. It's rumored some companies consider this effect so pronounced, that they intentionally leak content to file sharing networks to increase overall demand for the product, and 'illegal' copies embody a form of viral marketing. Thus we see two completely conflicting mathematical models for the same situation, without any way (yet) to determine the validity of either.
- Prior to breach notification laws, there were no losses to the attacked company associated with a data breach involving credit cards or personal information. Specifically, with compromised credit card numbers, the company losing the data suffered no impairment to its ability to perform transactions. Instead the cardholders and the issuing banks suffered financial losses. Thus a company performing a risk calculation using a value quantification model would see no reason to invest in protecting those cards. Data breach notification laws changed that equation by enforcing losses on the organization, but even those regulatory costs don't necessarily reflect the value of the data (as we'll discuss later, however, they do provide a good baseline).
- It's not uncommon for disgruntled sales executives leaving a company to gather up intellectual property ranging from pricing sheets to customer lists. Many of these individuals end up working for competitors, and use the data for their new employer. While they will focus their new sales efforts directly on customers of their old organization, this doesn't mean all (or any) of those customers will switch vendors, but it certainly increases the risk and alters the competitive situation. Any loss is impossible to measure until after the fact, and even then can't be used to accurately predict future losses under similar circumstances.

The complexities of information valuation

Data that has value is called *information*. The overall value of that information depends on its context — on how it's used, how often it is used, and how many people derive value from it. The value of information technology to any business is thus its ability to store, manage, present, analyze, and safeguard that data to support business operations, thus giving all those 0s and 1s value. Some types of data have inherent value: credit card numbers, social security numbers, military service records, and credit card transactional records all have value to the right audiences; as they support credit checks, employment verification, applications for loans, and insurance. Credit card numbers might be worth $1, and a social security number with associated name and address could be worth $5. Other types of data have derived value. Customer browsing and purchase histories used to market products during browsing sessions have value as they can have a direct impact on sales. Customer services, customer satisfaction, sales enticements, business analytics, and competitive differentiation derived from that data all have value. However, as we showed above, the ultimate value of the data is more complex and built from a composite of all these things; the more people within an organization who can access data and derive information from it, the move valuable the data is.

Why the value of information is always changing, and can't be completely measured.

Enterprise information is constantly examined, inserted, reported, compared, updated, and otherwise used. Seldom is collected data used for a single, specific purpose; rather the data is used by multiple people and business units to fulfill different needs. Data from different sources is combined and compared to derive value and other insights that assist people in getting their jobs done. This data is also shared with partners and customers, further increasing usage and value. Data changes every day; customer records grow stale over time and lose value, while others are augmented and

increase in value. New clients are added and new products are sold. The balance sheet changes and new expenses arise. Customer browsing histories, sales data, and marketing metrics are added; and additional metrics are derived. The data is always changing, so its value is always changing as well, for better and worse. Even the same piece of data holds different value in different contexts — *e.g.,* a credit card number without a corresponding name is little more than a 16 digit number. This makes analysis of the value of data an ongoing process with a moving target.

In the remainder of this document we will lay out our model, which has been designed to address the deficiencies we identified in other models. In the next section we will discuss the value of data to your organization, and how to balance disparate factors in a unified model.

Information Valuation Model

We know our data has value, but we can't assign a definitive or fixed monetary value to it. We want to use the value to justify spending on security, but trying to tie it to purely quantitative models for investment justification is impossible. We can use educated guesses but they're still guesses, and if we pretend they are solid metrics we're likely to make bad risk decisions. Rather than focusing on difficult (or impossible) to measure quantitative value, let's start our business justification framework with qualitative assessments. Keep in mind that just because we aren't quantifying the value of the data doesn't mean we won't use other quantifiable metrics later in the model. Just because you cannot completely quantify the value of data, that doesn't mean you should throw all metrics out the window.

To keep things practical, let's select a data type and assign an arbitrary value to it. To keep things simple you might use a range of numbers from 1 to 3, or 'Low', 'Medium', and 'High' to represent the value of the data. For our system we will use a range of 1-5 to give us more granularity, with 1 being a low value and 5 being a high value.

Another two metrics help account for business context in our valuation: frequency of use and audiences. The more often the data is used, the higher its value (generally). The audience may be a handful of people at the company, or may be partners & customers as well as internal staff. More use by more people often indicates higher value, as well as higher exposure to risk. These factors are important not only for understanding the value of information, but also the threats and risks associated with it — and so our justification for expenditures. These two items will not be used as primary indicators of value, but will modify an 'intrinsic' value we will discuss more thoroughly below. As before, we will assign each metric a number from 1 to 5 , and we suggest you at least loosely define the scope of those ranges. Finally, we will examine three audiences that use the data: employees, customers, and partners; and derive a 1-5 score.

The value of some data changes based on time or context, and for those cases we suggest you define and rate it differently for the different contexts. For example, product information before product release is more sensitive than the same information after release.

As an example, consider student records at a university. The value of these records is considered high, and so we would assign a value of five. While the value of this data is considered 'High' as it affects students financially, the frequency of use may be moderate because these records are accessed and updated mostly during a predictable window — at the beginning and end of each semester. The number of audiences for this data is two, as the records are used by various university staff (financial services and the registrar's office), and the student (customer). Our tabular representation looks like this:

Data	Value	Frequency	Audience
Student Record	5	2	2

Valuation examples

As a basic exercise, let's take a look at several common data types, discuss how they are used, and qualify their value to the organization. Several of these clearly have a high value to the organization, but others vary. Frequency of use and audience are different for every company. Before you start deriving values, you need to sit down with executives and business unit managers to find out what information you rely on in the first place, then use these valuation scenarios to help rank the information, and then feed the rest of the justification model.

Credit card numbers

Holding credit card data is essential for many organizations — a common requirement for dispute resolution; because most merchants sell products on the Internet, card data is subject to PCI DSS requirements. In addition to serving this primary function, customer support and marketing metrics derive value from the data. This information is used by employees and customers, but not shared with partners.

Data	Value	Frequency	Audience
Credit Card Number	4	2	3

Healthcare information (financial)

Personally Identifiable Information is a common target for attackers, and a key element for fraud since it often contains financial or identifying information. For organizations such as hospitals, this information is necessary and used widely for treatment. While the access frequency may be moderate (or low, when a patient isn't under active treatment), it is used by patients, hospital staff, and third parties such as clinicians and insurance personnel.

Data	Value	Frequency	Audience
Healthcare PII	5	3	4

Intellectual property

Intellectual Property can take many forms, from patents to source code, so the values associated with this type of data vary from company to company. In the case of a publicly traded company, this may be project-related or investment information that could be used for insider trading. The value would be moderate for the employees that use this information, but high near the end of the quarter and other disclosure periods, when it's also exposed to a wider audience.

Data	Value	Frequency	Audience
Financial IP (normal)	3	2	1
Financial IP (disclosure period)	5	2	2

Trade secrets

Trade secrets are another data type to consider. While the audience may be limited to a select few individuals within the company, with low frequency of use, the business value may be extraordinarily high.

Data	Value	Frequency	Audience
Trade Secrets	5	1	1

Sales data

The value of sales data for completed transactions varies widely by company. Pricing, customer lists, and contact information, are used widely throughout and between companies. In the hands of a competitor, this information could pose a serious threat to sales and revenue.

Data	Value	Frequency	Audience
Sales Data	2	5	4

Customer Metrics

The value of customer metrics varies radically from company to company. Credit card issuers, for example, may rate this data as having moderate value as it is used for fraud detection as well as sold to merchants and marketers. The information is used by employees and third party purchasers, and provided to customers to review spending.

Data	Value	Frequency	Audience
Customer Metrics	4	2	3

You can create more more categories, and even bracket dollar value ranges if you find that helpful in assigning relative value to each data type in your organization. But we want to emphasize that these are qualitative and not quantitative assessments, and they are relative within your organization rather than absolute. The point is to show that your business uses many forms of information. Each type is used for different business functions, and has its value to the organization, even if the value is not in dollars.

Next we will examine threats to this data, and derive measurements to put the risks into perspective.

Estimating Risk

Measuring and understanding the risks to information

If data security were a profit center, we could shift our business justification discussion from the value of information right into assessing its potential for profit. But since that isn't the case, we are forced to examine potential reductions in value as a guide to whether action is warranted. The approach we need to take is to understand the risks that directly threaten the value of data and the security safeguards that counter those risks. Security, in its many forms, is the primary method we use for managing risks to data so understanding both the information risks and security investments available to mitigate them is are essential prerequisites for our balancing act. In this section we'll discuss the risks and threats to our information, and in the next section we'll consider losses. When we pull the model together we will map potential data security investments against the possible value-based risks, losses, and benefits to derive the overall justification.

There's no question our data is at risk; from malicious attackers and nefarious insiders to random accidents and user errors, we read about breaches and loss nearly every day. Universities, governments, individuals, small and large businesses alike are constantly suffering information loss both public and private. But while we have an intuitive sense that data security is a major issue, we have trouble getting a handle on the real risks to data in a quantitative sense. The number of possible threats and ways to steal information is staggering, but when it comes to quantifying risks, we lack much of the information needed for an accurate understanding of how these risks impact us.

Combining quantitative and qualitative risk estimates

We'll take a different approach to looking at risk; we will focus on quantifying the things that we can, qualifying the things we can't, and combining them in a consistent framework. While we can measure some risks, such as the odds of losing a laptop, it's nearly impossible to measure other risks, such as a database breach via a web application due to a new vulnerability. If we limit ourselves only to what we can precisely measure, we won't be able to account for many real risks to our information. Inclusion of quantitative assessments, since they are a powerful tool to understand risk and influence decisions, help validate the overall model.

For our business justification model, we deliberately simplify the risk assessment process to give us just what we need to understand need for data security investments. Since different data types have different values, and each type faces different risks, risk analysis works best when performed for a particular information category, and is far less effective when used in a generic analysis. When we pull the model together in the final section we'll show you how to link the risk assessment to valuation, and when a generic assessment is still valid.

We start by listing out the pertinent risk categories, then the likelihood or annual rate of occurrence for each risk, followed by severity ratings broken out for confidentiality, integrity, and availability. For risk events we can predict with reasonable accuracy, such as lost laptops with sensitive information, we can use numbers. In the example below, we know the Annualized Rate of Occurrence (ARO), so we plug with value in. For less predictable risks, we just rate them from "low" to "high". We then mark off our currently estimated (or measured) levels in each category. For qualitative measure, we will

use a 1-5 scale to , but this is arbitrary, and you should use whatever scale that provides you with a level of granularity that assists understanding.

Remember that is evaluation is risk based; we'll cover potential loss measurements in the next section. While this might seem counterintuitive, it allows us to account for security controls that reduce potential losses from multiple risk categories and reduce complexity. Remember — we are focusing on business justification, not a comprehensive risk management system. We want to decouple these elements; otherwise every justification project would become a 2-year risk assessment.

Risk Estimation: Credit Card Data (Sample):

		Impact			
Risk	**Likelihood/ARO**	**C**	**I**	**A**	**Total**
Lost Laptop	43	4	1	3	51
Database Breach (Ext)	2	5	3	2	12

This is the simplified risk scorecard for the business justification model. The totals aren't meant to compare one risk category to another, but to derive estimated totals we will use in our business justification to show potential reductions from the evaluated investment. While different organizations face different risk categories, we've included the most common data security risks here, and in Section 6 we show how it integrates into the overall model.

Common data security risks

The following is an outline of the major categories for information loss. Any time you read about a data breach, one or more of these events occurred. This list isn't intended to comprehensive, rather provide a good overview of common data security risk categories to give you a jump start on implementing the model. Rather than discuss each and every threat vector, we will present logical groups to illustrate that the risks and potential solutions tend to be very similar within each specific category. The following are the principal categories to consider:

Lost Media

This category describes data at rest, residing on some form of media, that has been lost or stolen. Media includes disk drives, tape, USB/memory sticks, laptops, and other devices. This category encompasses the majority of cases of data loss. Typical security measures for this class includes media encryption, media 'sanitizing', and in some cases endpoint Data Loss Prevention technology.

- *Lost disks/backup tape:* Lost backup media is one of the largest causes of information loss. At any given moment losing media has a low probability, but as media lasts for a very long time, this risk persists unless mitigated. Safeguards: Media encryption and disk 'sanitizers', with both providing a very high degree of mitigation.
- *Lost/stolen laptop:* Data recovered from lost or stolen laptops is the preeminent threat to loss of data. The risk of losing laptops is very high. Safeguards: Full disk encryption provides a high degree of assurance. Policies to keep sensitive data off laptops have low effectiveness, but coupled with endpoint verification can provide a moderate degree of risk mitigation.
- *Information leaked through decommissioned servers/drives:* Sale of servers and components has resulted in a significant number of data breaches. Safeguards: Disk 'sanitizers', along with process modification so that these tools are used, are highly effective. Media encryption in earlier phases of the data lifecycle is equally effective.

- *Lost portable storage (memory stick/flash drive):* Small, capable of holding tremendous quantities of data, easy to use, and easy to lose. These remain one of the top ways data is lost. Safeguards: Providing employees with 'smart' memory sticks with built-in encryption is highly effective. DLP endpoint technologies that manage data moving on/off media provides reasonably effective control.
- *Stolen servers/workstations:* The theft of servers or workstations has a low probability when compared to lost media or laptops. If physical security is poor, the rate of theft naturally increases. The goal is typically sale of the equipment rather than the data — data theft is generally a byproduct. Safeguards: Physical security is typically the preferred approach, with a high degree of effectiveness. Full disk encryption has a high degree of effectiveness as well, but impacts performance.

Inadvertent Disclosure

This category includes data being accidentally exposed in some way that leads to unwanted disclosure. Examples include email to unwanted recipients, posting confidential data to web sites, unsecured Internet transmissions, lack of access controls, and the like. Safeguards include email & web security platforms, DLP and access controls systems. Each is effective, but only against certain threat types. Process and workflow controls are also needed to help catch human error.

- *Data accidentally leaked through email (Sniffed, wrong address, un-purged document metadata):* Mistakenly mailing lists of customers or intellectual property is a common occurrence, and intentional mailing of company secrets remains high despite most being aware that outgoing email is being scanned or audited. Safeguards: Email security products are moderately effective at detecting sensitive data in email streams, and most provide secure bridges for communicating with partners. Most tools are ineffective at discovering data sent to the wrong address.
- *Data leaked by inadvertent exposure:* (Posted to the web, open file shares, unprotected FTP, or otherwise placed in an insecure location): One of the most difficult challenges is to catch errors and mistakes by people who are tasked with data processing efforts. Accidental postings can be addressed through policy and workflow controls, and for some types of events, DLP.
- *Data leaked by unsecured connection:* Information sniffed for correspondence or transactions that were meant to be secured, but were routed over the Internet. Many such leaks are caused by errors in internal configuration and unintentional, and employees are typically unaware of the issue. Safeguards: Most email and web security platforms provide secure bridging and routing of correspondence, and are effective when properly configured. Process changes to include periodic review that routing to secured networks is set up properly is also effective.
- *Data leaked through file sharing:* File sharing programs are used to move large files efficiently (and possibly illegally). Because they are illegal, they are often surreptitiously installed and used, which prevents security personnel from reviewing configuration and ensuring business files are not also (unintentionally) shared. Data loss via this method is typically intentional. Safeguards: Policies for not allowing file sharing programs can deter some occurrences. Web security platforms, when combined with strong network security, are effective at detecting and blocking these products.

External Attack/Breach

This category describes instances of data theft where company systems and applications are compromised by a malicious attacker, affecting confidentiality and integrity. Typical attacks include compromised accounts/passwords, SQL Injection, web site attacks, trojans, viruses, network 'sniffers' and others. Successful compromise often results in installation of additional malicious code. While not the most frequent, this category includes the most damaging data breaches and is most likely to be result in fraud. Any security precautions may assist in detection; but assessment, penetration testing, data encryption, and application security are common preventative controls; with application & database monitoring, WAF, and flow based detection popular as detective controls.

- *Data theft through compromised account (weak passwords):* Accounts compromised after the password is guessed Safeguards: Requirement of strong passwords. Process mandates of cycling passwords. Blocking account access after X number of failed log-ins. Some access control systems can force strong passwords and automate password policy enforcement with a reasonably high degree of success, and many penetration testing tools can identify accounts with weak passwords.
- *Network/systems breach:* The organization is compromised via a traditional external attack, which is then used to target data. An example is a network breach followed by installation of a "sniffer" to collect credit card numbers in a financial transaction pathway. Defenses include traditional perimeter security controls, and outbound data security such as DLP.
- *Database breach:* Databases are extraordinarily complex applications. The term 'database breach' applies to many different types of attacks on a database server. Specific attack vectors may include misuse of privileges, misused features, buffer overflow and SQL injection. The typical goal of a database attack is to steal the information contained within the database. Injection of arbitrary code into the database to alter its intended function, or even use the database as a platform to launch attacks on other applications is also common, but calls for the same protective measures. Safeguards: Database Application Monitoring to detect attacks and misuse. Database Vulnerability Assessment. DAM is used to monitor use of the database and is a detective control by nature. DAM examines queries made against the database, compares each query against known threat patterns and business best practices, and reacts to suspicious events. Vulnerability Assessment is a preventative methodology that examines the database for known vulnerabilities and weaknesses in the configuration, setup, and use of the database.
- *Web application breach (logic flaw, exploit):* This category includes any attack on the web application that serves the data to its intended audience. Misuse of the web application platform, alteration of session information from the browser, buffer overflows, and SQL injection through the web application, are all common exploits. Vulnerability Assessment and Penetration Testing provides a high degree of security from data leakage through both logic flaws and insecure programming. Additional measures can be taken through infrastructure protection, as well as modification of the web application code.
- *Breach via compromised endpoint:* One effective method of attack is to compromise an internal system/endpoint, then use it to both extract data locally and attack additional systems. Standard endpoint security practices address this risk.

Malicious Insider

This category describes instances of data theft where company systems and applications are compromised by a malicious insider, affecting confidentiality and integrity. Insider threats are particularly hard to control since employees, contractors, and other insiders are trusted and we're often trying to detect when they perform an authorized action, with malicious intent. Insiders without authorized access are controlled via standard data security controls (access controls, encryption). Malicious activity with authorized access can be managed with policy-based data security tools such as DLP and Database Activity Monitoring.

- *Data breach through portable storage (USB drives, CD/DVD):* A malicious insider transfers sensitive data onto portable storage for inappropriate use. Manage using endpoint DLP or portable device control.
- *Data breach through personal email/web:* The malicious insider uses a web based email service (e.g. Hotmail), web storage service, or personal FTP site to send the data outside the organization for later collection. This can be limited using web filtering and DLP.
- *Database breach by insider (employee, partner, contractor):* All users of a database have credentials to use it, but between roles, groups, and specific user credentials, it is common for users to have permissions to perform actions they should not. Database administrators typically have rights credentials to do anything with the database, but in reality should be allowed only a small subset of the total functionality. While this threat is similar to others mentioned in

this section, these breaches more closely resemble normal transactions, and thus be much more difficult to detect. Vulnerability Assessment and penetration testing tools can detect excess permissions; activity monitoring and auditing technologies detect misuse.

Potential Losses

Understanding Potential Losses

Earlier we deliberately decoupled potential losses from risk impact, even though loss is clearly the result of a risk incident. Since this is a business justification model rather than a risk management model, it allows us to account for major types of potential loss that are the result of multiple types of risk and simplifies our overall analysis. We will highlight the major loss categories associated with data security, and as with our risk estimates, break them out into quantitative and qualitative categories. These loss categories can be directly correlated back to risk estimates, and it may make sense to walk through that exercise at times, but as we complete our business justification you'll see why it isn't normally necessary.

If data is stolen in a security breach, will it cost you a million dollars? A single dollar? Will you even notice? Under "Data Loss Models", we introduced a method for estimating to the value of the data that your company possess to underscore what is at stake. Now we will provide a technique for estimating the costs to the business in the event of a loss. We look at some types of loss and their impacts. Some of these have hard costs that can be estimated with a reasonable degree of accuracy. Others are more nebulous so assigning monetary values doesn't make sense. But don't forget that although while we may not be able to fully quantify these losses, we cannot afford to ignore, them because unquantifiable costs can be just as damaging.

Quantified vs. Qualified Losses

As we discussed with noisy threats, it is much easier to justify security spending based on quantifiable threats with a clear impact on productivity and efficiency. With data security, quantification is often the rare exception, and real loss a typically combination of quantified and qualified elements. For example, a data breach at your company may not be evident until long after the fact. You don't lose access to the data, and you might not suffer direct losses. But if the incident becomes public, you could then face regulatory and notification costs. Stolen customer lists and pricing sheets, stolen financial plans, and stolen source code can all reduce competitive advantage and impact sales — or not, depending on who stole what. Data stolen from your company may be used to commit fraud, but the fraud itself may be committed elsewhere. Customer information used in identity theft causes your customers major hassles, and if they discover your firm was the source of the information, you may face fines and legal battles over liability. As these can account for a majority of total costs, despite the difficulty in obtaining an estimate of the impact, we must still account for the potential loss to justify spending to prevent or reduce it.

There are two approaches to combining quantified and qualified potential losses. In the first, you walk through each potential loss category and either assign an estimated monetary value, or rate it on our 1-5 scale. This method is faster, but doesn't help correlate the potential loss with your tolerance. In the second method, you create a chart like the one below, where all potential losses are rated on a 1-5 scale, with either value ranges (for quantitative loss) in the cells, or qualitative statements describing the level of loss. This method takes longer, since you need to identify five measurement

points for each loss category, but allows you to more easily compare potential losses against your tolerance, and identify security investments to bring the potential losses (or their likelihood) down to an acceptable level.

Loss	1	2	3	4	5
Notification costs (total, not per record)	$0-$1000	$1,001-$10,000	$10,001-$100,000	$100,001-$500,000	>$500,000
Reputation Damage	No negative publicity	Single negative press mention, local/online only	Ongoing negative press <2 weeks, local/online only, Single major outlet mention.	Ongoing sustained negative press >2 weeks, including multiple major outlets. Measurable drop in customer activity.	Sustained negative press in major outlets or on a national scale. Material drop in customer activity.

Potential Loss Categories

Here are our recommended assessment categories for potential loss, categorized by those we consider quantifiable vs. only qualifiable:

Quantifiable potential data security losses:

- *Notification Costs:* CA 1386 and associated state mandates to inform customers in the event of a data breach. Notification costs can be estimated in advance, and include contact with customers, as well as any credit monitoring services to identify fraudulent events. The cost is linear with the total number of records compromised.
- *Compliance Costs:* Most companies are subject to federal regulations or industry codes they must adhere to. Loss of data and data integrity issues push them out of compliance. HIPAA, GLBA, SOX, and others include data verification requirements with fines for failure to comply
- *Investigation & Remediation Costs:* An investigation into how the data was compromised, and the associated costs to remediate the relevant security weaknesses, have a measurable cost to the organization.
- *Contracts/SLA:* Service level agreements about quality or timeliness of services are common, as are confidentiality agreements. Businesses that provide data services rely upon the completeness, accuracy, and availability of data; falling short in any one area can violate SLAs and/or subject the company to fines or loss of revenues.
- *Credit*: Loss of data and compromise of IT systems are both viewed as indications of investment risk by the financial community. The resulting impact on interest rates and availability of funds may affect profitability.
- *Future Business & Accreditation:* Data loss, compliance failures, or compliance penalties may preclude your ability to bid on contracts or even participate in certain ventures due to loss of accreditation. This can be a permanent or temporary loss, but the effects are tangible. Note that future business is also a qualitative loss — here we refer to definitive measurements, such as exclusions from business markets, as opposed to potential losses due to customer loyalty/concern.
- *Continuity of Business:* Denial of Service impacts customers service and loss of business while data or systems are unavailable. These are often measurable for transaction-based businesses.

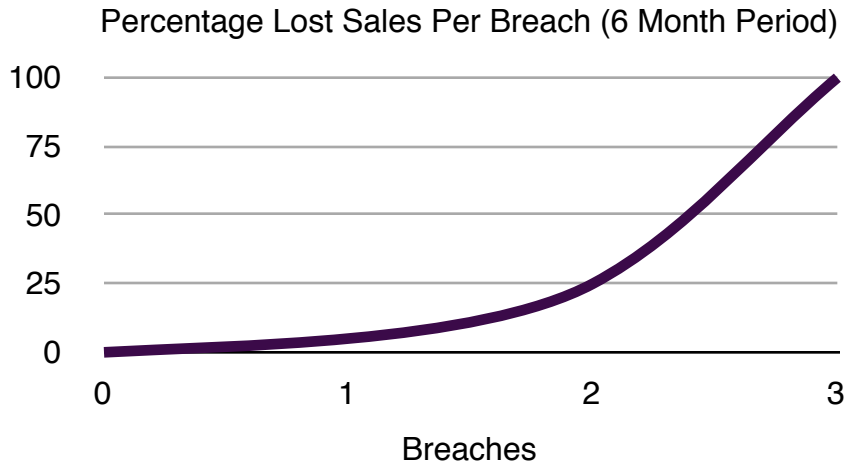
Qualifiable potential data security losses:

- *Reputation Damage:* The reputation of a company affects its value in a number of ways. New customers often seek out firms they know and trust. Investors are likely to buy stock from companies which are trustworthy and operate effectively. Risks to reputation affect both, but it's generally impossible to attribute an impact to a single event, because other events, non-risk factors, and general market forces all feed into customer behavior.
- *Customer Loyalty:* How the data loss is perceived by customers has an effect on customer and brand loyalty. If the loss of the data is viewed as preventable, and the inconvenience or financial cost to customers is high, some customers will stop doing business with the company.
- *Loss of Sales:* Your customer contact information and pricing sheets in the hands of your competitor provide ample data for targeted sales campaigns. Any successes come at your expense.
- *Competitive Advantage:* R&D expenditure to create a new and competitive product can be devalued if that research, source code, process, or ingredient list is stolen; but since you aren't blocked from still bringing the product to market the lost benefit is not fully quantifiable.
- *Future Business:* You cannot accurately predict lost future business, unless you restrict it to market/ecosystem/contract exclusion as we mentioned above. We've seen single breach disclosures put a company out of business, while other companies see sales growth despite major public breaches.

Exponential loss growth

While a single incident might result in minimal losses, a string of ongoing incidents will likely exponentially increase your losses — especially in qualitative areas such as reputation damage and loss of future business.

Despite what most of the surveys claim, there is very little evidence of correlation between a single data breaches and lost business, or even stock price. For example, TJX suffered one of the largest data breaches in history, but sales increased steadily through the incident. It's clear customers either didn't pay attention, or felt that the security controls implemented after the incident made TJX safer to shop. But if TJX suffered an ongoing string of data breaches over a period of months, at some point there would be material loss of business.



When providing a business justification for security spending, you do not need to account for every single aspect of loss. Nor do you need to even show that the majority of data value is at risk. Instead, you need to understand that valuable data is at risk, and examine the potential benefits of security and the reduction of loss in relation to the cost of the investment. Real damages may be small, but the potential for loss is considerable. If it can be shown that mitigating the risk vector associated with data theft also accomplishes operational goals, the argument is even stronger. If the

investment also accounts for compliance controls, or makes a business process more efficient, the effort may pay for itself.

Additional Positive Benefits

Cost savings and other positive benefits

We have discussed how to assess both the value of the information your company uses, and some potential losses should your data be stolen. The bad news is that security spending mitigates some portion of the threats, but cannot eliminate them. While we would like our solutions to eradicate threats, it's usually more complicated. The good news is that security spending commonly addresses other areas of need. The collection, analysis, and reporting capabilities built into most data security products — when used with a business processing perspective — supplement existing applications and systems. For example, security investment can readily be leveraged to reduce compliance costs, improve systems management, efficiently analyze workflows, and gain a better understanding of how data is used and where it is located. This consistently results in greater utility along with reduced cost of ownership via automation. We will discuss each of these in greater detail, and how the secondary benefit creates an added variable in the analysis.

Reduced compliance/audit costs

Regulatory initiatives require that certain processes be monitored for policy conformance, as well as subsequent verification to ensure those policies and controls align appropriately with compliance guidelines. As most security products examine business processes for suspected misuse or security violations, there is considerable overlap with compliance controls. Certain provisions in the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), and the Health Insurance Portability and Accountability Act (HIPPA) either call for security, process controls, or transactional auditing. While data security tools and products focus on security and appropriate use of information, policies can be structured to address compliance as well.

Let's look at a couple ways security technologies assist with compliance:

- Filtering, analysis, and reporting help reduce audit costs by providing auditors with necessary information to quickly verify the efficacy and integrity of controls; gathering this information is typically an expensive portion of an audit. This is the single most effective way data security tools reduce audit costs, and savings may be substantial.
- Access controls assist with separation of duties between operational, administrative, and auditing roles.
- Email security products provide with Safeguards Rule and Pretexting protection as required by GLBA.
- Activity Monitoring solutions perform transactional analysis, and with additional polices can provide process controls for end-of-period-adjustments (SOX) as well as address 'safeguard' requirements in GLBA.
- Security platforms separate the roles of data collection, data analysis, and policy enforcement, and can direct alerts to appropriate audiences outside security.
- Collection of audit logs, combined with automated filtering and encryption, address common data retention obligations.
- DLP, DRM, and encryption products assist in compliance with HIPAA and appropriate use of student records (FERPA).

- DLP tools, using content discovery, identify the locations of sensitive data to reduce manual discovery/audit time, and can provide reports for internal remediation or external auditors.
  - These same tools can reduce audit scope by identifying which systems contain regulated information, and excluding those that don't.
- Auditing technologies provide a view into transactional activity, and establish the efficacy and appropriateness of controls.

Reduced TCO

Data security products collect information and events that have relevance beyond security. By design they provide a generic tool for the collection, analysis, and reporting of events that serve regulatory, industry, and business processing controls; automating much of the analysis and integrating with other knowledge management and response systems. As a result they can enhance existing IT systems in addition to their primary security functions. The total cost of ownership is reduced for both security and general IT systems, as the two reinforce each other — possibly without requiring additional staff. Let's examine a few cases:

- Automating inspection of systems and controls on financial data reduces manual inspection by Internal Audit staff.
- Systems Management benefits from automating tedious inspection of information services, verifying that services are configured according to best practices; this can reduce breaches and system downtime, and ease the maintenance burden.
- Security controls can ensure business processes are followed and detect failure of operations, generating alerts in existing trouble ticketing systems.
- DLP tools, using content discovery, can reduce the scope of required security controls by identifying the locations of covered information, and excluding other locations which don't require the same degree of security.

Risk reduction

Your evaluation process focuses on determining if you can justify spending some amount of money on a certain product or to address a specific threat. That laser focus is great, but data security is an enterprise issue, so don't lose sight of the big picture. Data security products overlap with general risk reduction, similar to the way these products reduce TCO and augment other compliance efforts. When compiling your list of tradeoffs, consider other areas of risk & reward as well.

- Assessment and penetration technologies discover vulnerabilities and reduce exposure; keeping data and applications safe helps protect networks and hosts.
- IT systems interconnect and share data. Stopping threats in one area of business processing can improve reliability and security in connected areas.
- Discovery helps analysts process and understand risk exposure by providing locating data, and recording how it is used throughout the enterprise, and ensuring compliance with usage policies.

Using data security to prioritize other investments

We are providing a model to help you justify security expenditures, but that doesn't mean our goal is to promote security spending. Our approach is pragmatic, and if you can achieve the same result without additional security products to support your applications, we are all for that. In much the same way that security can reduce TCO, some products and platforms have security built in, thus avoiding the need for additional security expenditures. We recognize that data security choices typically are the last to be made, *after* deployment of the applications for business processing, and after infrastructure choices to support the business applications. When evaluating platforms, both intrinsic data security capabilities and ease of integration with existing data security infrastructure should be part of any analysis and proof of

concept processes. Web application servers, database servers, and various enterprise application platforms are routinely evaluated for functionality and support for different development and operating environments, but security is often an afterthought. Keep in mind that adding security to an application or platform after purchase (or even after deployment) can be very expensive, as you are probably aware if you are reading this document and engaged in this exercise. We strongly suggest you keep data security in general, and the specific considerations outlined here, in mind when you evaluate new applications for data processing, and take note of where products fall short. Forethought during the buying process can save money and avoid headaches in the long run.

Business Justification

Building the business justification

Now that we've discussed the different business justification elements, it's time to pull them together into a complete process. We'll use one of two options, depending on what is driving the project:

- Investment-based justification is for evaluating a particular technology, process change, or other investment, with a nebulous protection goal. For example, "we are thinking about investing in DLP".
- Goal-based justification is for solving a particular problem. For example, "we need to protect our credit card numbers to comply with PCI." Note that a goal-based justification model can only be used once you've selected a technology, process, or other investment — it isn't meant to help you find the right tool for the job, rather to evaluate tools already under consideration.

Since goal-based projects are more constrained in terms of scope, we will walk through the investment-based process in depth, and then show you how to modify it for a goal-based project.

We've included a sample Data Security Business Justification Worksheet in Appendix A, and it may be helpful to pull that out as we walk through the process.

Pre-Evaluation

If you anticipate evaluating multiple data security options, or you are building a data security strategy, we recommend you perform the data valuation, risk estimate, and potential loss estimate before proceeding with any further business justification or evaluation. This will provide you with essential information you can leverage across multiple projects, including product evaluations and planning your data security strategy, or even to assist with risk evaluations.

- Data Valuation: Working with business unit heads and other management, list major information/data types and complete the valuation as described earlier. Then stack-rank based on sensitivity to help ensure any data security investments are aligned with enterprise priorities.
- Risk Estimate: Start with the data security risk categories included here, then add or remove to meet your own operational, regulatory, and contractual requirements. Then perform the risk assessment — since some risk categories don't necessarily align with a specific data type, you can either perform risk estimates for all data types or a subset, limit it to broad categories (*e.g.,* PII and Intellectual Property), or default the analysis to the most sensitive information exposed to that potential risk. Our suggestion is to perform a risk estimate for your 3-5 most sensitive data types.
- Loss Estimate: Start with the potential loss categories included in this report, and adjust as needed to match your own operational, regulatory, or contractual profile. As with the risk estimate; you can perform an in-depth analysis or restrict your loss estimate to major critical data types, broad categories, or the most sensitive data exposed to each potential loss.

Step 1: Define the product/technology, process, or investment

List the specific product, technology, process change, or investment (*e.g.,* business partnership, service, or new hire) and a brief description, including what business problem is solved (only use technical descriptions if the justification is intended for a technical audience).

List any cost estimate; either a monetary amount or Full-Time Equivalents required.

Investment	Cost	Description

Step 2: Map the investment to covered data types and valuation

Detail which data types are potentially protected by the investment; and the valuation, frequency, and audience for each data type. These should be stack ranked, with the most valuable data at the top. Do not list data types the investment doesn't protect, unless you are deliberately highlighting security gaps.

This step is the acid test before continuing further. If the investment doesn't protect desired or expected data types, it isn't a good match and should be discarded. A description area is included on the worksheet to provide an overview of how/why the potential investment addresses the listed data types.

Data Type	Value	Frequency	Audience

Step 3: Determine the potential risk reduction capability of the investment

Perform a risk estimate for the covered data types, then adjust the estimate for your expectations if the potential investment is implemented. Depending on your goals, you may need to perform this for different data types, focus on a single data type, or perform a quicker but less precise generic analysis.

		Impact				
Risk	Likelihood/ARO	C	I	A	Total	% Δ

			Impact								
	before	after	B	A	B	A	B	A	B	A	

This shows estimated risk reduction capabilities for the potential investment. In the description area provide an overview of how and why risk is reduced, with an emphasis on either the largest reductions, or reductions of key risk concerns.

Step 4: Determine the potential loss reduction capability of the investment

Perform a potential loss estimate for the covered data types, then adjust the estimate for your expectation if the investment is implemented. Depending on your goals, you may need to perform this for different data types, focus on a single data type, or perform a quicker but less precise generic analysis.

If you already performed a complete potential loss analysis, instead of carrying over the complete table you can just list the deltas (changes).

Loss	1	2	3	4	5	B	A

This provides the estimated loss reduction capabilities for the investment. In some cases the result will be a quantitative monetary value; in others it will be a qualitative reduction. In the description area on the worksheet, detail the most pertinent potential loss reductions, and how and why the product provides them.

Step 5: Detail additional benefits provided by the investment

Detail other possible benefits of the data security investment, including both quantitative and qualitative results.

Benefit	Description	Est. Value ($)

Step 6: Summarize the business justification

Now that you've completed the worksheet, you have a summary of what the potential investment is, what data it protects, how it reduces risk, how it reduces potential loss, and any other benefits. Use this information to detail a summary, and only use technical language if you are absolutely certain the justification is for a technical manager. We highly suggest you focus on the most important benefits, as opposed to including everything — you can always attach your completed worksheet and its more detailed analysis if appropriate.

Here are some examples of effective business justifications:

- Investing in DLP content discovery (data at rest scanning) will reduce our PCI related audit costs by 15% by providing detailed, current reports of the location of all PCI data. This translates to $xx per annual audit.
- Last year we lost 43 laptops, 27 of which contained sensitive information. Laptop full drive encryption for all mobile workers effectively eliminates this risk. Since Y tool also integrates with our systems management console and tells us exactly which systems are encrypted, this reduces our risk of an unencrypted laptop slipping through the gaps by 90%.
- Our SOX auditor requires us to implement full monitoring of database administrators of financial applications within 2 fiscal quarters. We estimate this will cost us $X using native auditing, but the administrators will be able to modify the logs, and we will need Y man-hours per audit cycle to analyze logs and create reports. Database Activity Monitoring costs %Y, which is more than native auditing, but by correlating the logs and providing the compliance reports it reduces the risk of a DBA modifying a log by Z%, and reduces our audit costs by 10% — a net potential gain of $ZZ, with better security as a secondary benefit.
- Installation of a full DLP suite reduces the chance of protected data being placed on a USB drive by 60%, the chances of it being emailed outside the organization by 80%, and the chance an employee will upload it to their personal webmail account by 70%.

Investment vs. Goal-Based Assessments

In a goal-based assessment you can reduce the scope of your evaluation to just those aspects of the defined goal affected by the potential investment. For example, if your goal is to protect credit card data in a database, limit your analysis to only that single data type, and only those potential risks and losses associated with credit cards in databases.

In an investment-based assessment your scope is likely wider because you are finding all potential data security benefits of the product — which may span multiple data types, risks, loss categories, and other benefits.

Conclusion

Justification of data security expenditures is a difficult challenge: whether or not to spend, and if so how much and where, are difficult questions. Data Security warrants a critical evaluation, but the multi-faceted issues around information security cannot be captured in ROI calculations. Typical benefit calculations are inadequate to address the complexities involved, and do not provide meaningful guidance for common questions like "Should I invest in this product?" If you feel you need a hard bottom line number, pick up a copy of Hitch-Hiker's Guide to the Galaxy for its answer. If you want a meaningful evaluation of the choices available to you, follow our model. You will have to do a little digging in order to come up with some of the data that is relevant to your organization and make some tough choices, but the framework provided will help walk you through the process.

The goal of this report is to help you analyze the important factors when building a business justification for data security expenditures. *We need to stress that this is not intended to promote blind spending,* but provides a method for comparative analysis between choices. On a more basic level, our goal is to provide pragmatic advice on complicated questions regarding IT expenditures. Your question may be something like "Do I invest in X or Y technology to address my security issue?", or "Is this a cost effective way to address ABC compliance issue?" To help answer these questions, we needed to look at the problem in a different way. Rather than coax a bottom line dollar cost from an equation, we boiled down the problem to its basic elements and then assess these factors in your specific situation. The end result can be used in and of itself, but we recommend comparing different solutions against one another, or one set of choices against another, as the results might surprise you.

This guide is intended to be used strategically. While we are boiling down the problem into specific elements of value and risk to provide the best estimates possible, don't get mired in the nuts and bolts of a specific technology or problem. It is our hope that you will use the framework for a broader examination of the available choices. Information security investment decisions are rarely centered on a single product or problem, so the worksheet is designed to be flexible enough to account for multi-factored analysis. We anticipate that you will find this guide helpful enough to apply to existing investments that combat 'noisy' problems, and determine whether to continue those investments or reinvest in other areas.

One final recommendation is to keep copies of your analysis and revisit the calculations on occasion. You will find that some of the comparisons are based upon purely qualified data, or information that you may identify as volatile. Threats, goals, the value of the data, and your tolerance for risk all vary over time; and you will often find better ways of quantifying some of these factors. The result is that your analysis will gradually grow stale. Periodic re-assessment is necessary to make sure you remain on track, revalidate your goals, and adjust the expectations of your organization if necessary.

Data Security Business Justification Worksheet

Step 1: Define the product/technology, process, or investment

List the specific product, technology, process change, or investment (e.g., business partnership, service, or new hire) and a brief description, including what business problem is solved (only use technical descriptions if the justification is intended for a technical audience).

List any cost estimate — either monetary amount or full time equivalents required.

Investment	Cost	Description

Step 2: Map the investment to covered data types and valuations

Detail which data types are potentially protected by the investment; and the valuation, frequency, and audience for each data type. These should be stack ranked, with the most valuable data at the top. Do not list data types the investment doesn't protect, unless you are deliberately highlighting security gaps.

Data Type	Value	Frequency	Audience	Rank

Description

Step 3: Determine the potential risk reduction capability of the investment

Perform a risk estimate for the covered data types, then adjust the estimate for your expectations if the investment is implemented. Depending on your goals, you may need to perform this for different data types, focus on a single data type, or perform a less accurate but more rapid generic analysis.

			Impact								
Risk	**Likelihood/ARO**		**C**		**I**		**A**		**Total**		**% Δ**
	before	after	B	A	B	A	B	A	B	A	
Inadvertent exposure											
Email leak											
Unsecured connection											
File sharing leak											
Compromised account											
Database breach											
Network/systems breach											
Misused privileges											
Web application breach											
Compromised endpoint											
Lost disk/tape											
Lost/stolen laptop											
Decommissioned media											
Lost portable storage											
Stolen workstation/server											
Insider- portable storage											
Insider- email/web											
Insider- database											

Description

Step 4: Determine the potential loss reduction capability of the investment

Perform a potential loss estimate for the covered data types, then adjust the estimate for your expectation if the investment is implemented. Depending on your goals, you may need to perform this for different data types, focus on a single data type, or perform a less accurate but more rapid generic analysis.

If you already performed a complete potential loss analysis, instead of carrying over the complete table you can just list the deltas (changes).

Loss	1	2	3	4	5	B	A
Notification costs							
Compliance costs							
Investigation and remediation costs							
Contracts/SLAs							
Credit							
Future business & accreditation							
Continuity of business							

Loss	1	2	3	4	5	B	A
Reputation damage							
Customer loyalty							
Loss of sales							
Competitive advantage							
Future business							

Description

Step 5: Detail additional benefits provided by the investment

Detail other possible benefits of the data security investment, including both quantitative and qualitative results.

Benefit	Description	Est. Value ($)
Reduced compliance costs		
Reduced audit costs		
Reduced TCO		
Additional risk reduction		

Description

Step 6: Business Justification Summary

Summarize the key benefits you expect to realize from the potential investment, including the information it protects, risk reduction capabilities, potential loss reduction, and additional positive benefits.

About

About the Authors

Rich Mogull, Founder

Rich Mogull has over 17 years experience in information security, physical security, and risk management. Prior to founding Securosis, Rich spent 7 years as one of Gartner's leading security analysts, where he advised thousands of clients, authored dozens of reports, and was consistently rated one of Gartner's top international speakers. He is well known for his work on data security technologies and has covered issues ranging from vulnerabilities and threats, to risk management frameworks, to major application security. Rich is the Security Editor of TidBITS, a monthly columnist for Dark Reading, and a frequently contributor to publications ranging from Information Security magazine to Macworld.

Adrian Lane, Senior Security Strategist

Adrian Lane is a Senior Security Strategist with 22 years of industry experience, bringing over a decade of C-level executive expertise to the Securosis team. Mr. Lane specializes in database architecture and data security. With extensive experience as a member of the vendor community, including positions at Ingres & Oracle; as well as an IT customer in the CIO role; Adrian brings a business-oriented perspective to security implementations. Prior to joining Securosis, Adrian was CTO at the database security firm IPLocks, where he was responsible for product & technology vision, market strategy, PR, and security evangelism. Mr. Lane also served as Vice President of Engineering at Touchpoint, for three years as CIO of the brokerage CPMi, and for two years as CTO of the security and digital rights management firm Transactor/Brodia. Mr. Lane is a Computer Science graduate of the University of California at Berkeley with post-graduate work in operating systems at Stanford University.

About Securosis

Securosis, L.L.C. is a security consulting practice dedicated to thought leadership, objectivity, and transparency. Our consultants have all held executive level positions and are dedicated to providing the highest value strategic consulting available.

We provide services in four main areas:

- Publishing and speaking: Including independent, objective white papers, webcasts, and in-person presentations.
- Strategic consulting for vendors: including market and product analysis and strategy, technology guidance, product evaluations, and merger and acquisition assessments.
- Strategic consulting for end users: including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessments.
- Investor consulting: technical due diligence including product and market evaluations, available in conjunction with deep product assessments with our research partners.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, startups, mid-sized enterprises, and major security vendors.

Securosis has partnered with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis.

About the SANS Institute

SANS is the most trusted and by far the largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost the largest collection of research documents about various aspects of information security and operates the Internet's early warning system — the Internet Storm Center.

Many of the valuable SANS resources are free to all who ask. They include the very popular Internet Storm Center, a weekly news digest (NewsBites), a weekly vulnerability digest (@RISK), flash security alerts, and more than 1,200 award-winning original research papers.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced