A CMI/SkyView Partners Business Brief White Paper:

Protecting Your Data—How Much Security is Enough?

By Carol Woodbury
President, SkyView Partners, Inc.

In Cooperation With
SKYVIEW PARTNERS, INC

CMI (Chouinard & Myhre, Inc.)
655 Redwood Hwy, Ste. 102
Mill Valley, CA 94941
415.480.3636
www.cm-inc.com

As organizations become increasingly aware of the need to protect their data the question that needs to be answered is — how much security is enough? Unfortunately, that's one of those 'it depends' questions. Each organization must consider their own requirements before confidently answering that question. This document discusses those considerations.

The answer to 'How much Security is Enough?' all depends on the data that the organization possesses. And then what must be considered is: does the data fall under any regulatory requirement and how valuable is the data to the organization. Let's consider these points.

Regulatory Compliance Requirements

When working with organizations one area we help our clients with is to think about the types of data they have throughout their organization. Examples include customer information, financial information (accounts receivable / accounts payable), inventory, human resource information and so forth.

Once you've taken inventory of the data retained throughout your organization, the first consideration to make is whether the data falls under any laws or regulations that impose specific security requirements. Obvious examples include credit cards which fall under the requirements of the Payment Card Industry's Data Security Standard (PCI DSS), financial data that falls under BASEL III, the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX) or the Japanese version (J-SOX) as well as private data that falls under Personal Information Protection and Electronics Document Act (PIPEDA), The Companies Bill or U.S. State breach notification laws. Many of these laws and regulations have specific data security requirements so it can be fairly easy to determine at least the minimum amount of security and the types of protection one needs to take to protect this type of data. For example, PCI DSS has specific requirements for what credit card information can be stored and the fact that it must be transmitted and stored encrypted.

But are security requirements stipulated in these laws and regulations always sufficient to protect data? No. Some laws and regulations stipulate that the data must be secured but provide no specific guidance or requirements for the exact steps you need to take to secure the data.

So how do you determine 'how much is enough' in these cases? The answer is to look at the intent of what is trying to be accomplished. Take SOX for example, the intent of this U.S. law is to ensure that the financial information of the company is accurate and can be relied upon. What does this mean in terms of security? At a minimum, that the access control settings of the databases containing financial data (along with any other data that directly feeds into the financials) enforce the appropriate role-based access. That is, those roles that have responsibility to update the financial data be allowed to do so while all other roles have read-only or are denied access altogether.

CMI (Chouinard & Myhre, Inc.)
655 Redwood Hwy, Ste. 102
Mill Valley, CA 94941
415.480.3636
www.cm-inc.com

On the surface, this may seem like an easy and obvious task. Only provide access to the application to the users of that application and customize—by role—what tasks users are allowed to perform within the application. That's one step. The other step is to make sure that the access rights to the database where the data is stored are set properly. Many application providers and security administrators ignore this step, leaving data directly accessible via ODBC or FTP connections by users without a business need to access the data. Depending on the access control setting, these users may be able to just read the data. But some application providers and internal developers leave the access set such that users have the ability to modify the data or delete records. An access control setting that allows users to modify or delete data from outside of the application's logic is a clear and obvious violation of many laws and regulations. This setting needs to be corrected—not only to come into compliance with these laws and regulations–but also to ensure the data is sufficiently protected so that your organization can rely on the integrity of the data.

Value to the Organization

The next consideration to make in your determination of 'how much is enough' is to determine the value of the data to the organization. This consideration is often overlooked and therefore, valuable data is often left with inadequate or non-existent protection measures. Most organizations fail to consider how valuable their data is to the overall organization. Consider some examples: a specialty retailor whose vendor list, in the hands of their competitors, would eliminate the uniqueness of their inventory; a non-profit organization who's mission is 'politically incorrect' has their donor list stolen and names are published on the Internet, sales data upon which commissions and bonuses are calculated is modified by an unscrupulous employee, pricing information is sold to a competitor in a business whose margins are extremely thin.

The data in these examples doesn't fall directly under any law or regulation yet it needs to be protected as the valuable asset that it represents.

Data Confidentiality

Laws and regulations require some types of data be kept confidential—healthcare information and credit card numbers are obvious examples. This requirement demands that—if you do nothing else—the default access control setting on the files and directories containing this information is set to 'deny by default.' It also makes sense that some non-regulated data—bank account, Social Security and Social Insurance numbers for example—also be kept confidential or private. But don't stop with the obvious. Think through the other data retained by your organization. You may want to keep financial information restricted to only selected employees. Or some organizations don't share sales quotas or pricing information between regions.

CMI (Chouinard & Myhre, Inc.)
655 Redwood Hwy, Ste. 102
Mill Valley, CA 94941
415.480.3636
www.cm-inc.com

Bottom line is that the appropriate access controls will ensure that data is only available to the approved users

Data Integrity

Data Integrity is often overlooked when considering how much security is enough. Consider how the results of queries or data warehouse analysis is part of your business processes. Orders are placed for additional supplies based on inventory numbers. Forecasts are made based on sales trends. Bonuses are calculated based on sales. If these numbers used as input to these formulas aren't accurate, payouts will be off. But worse, significant business decisions could be made based on inaccurate data that affects the bottom line of your organization.

Not all data is confidential and needs to be secured with an access control of 'deny by default.' However, having access control settings that ensure the integrity of the data (at most 'read only') on the databases and directories where data is stored should be a fundamental tenant of all organizations. Otherwise, the accuracy of the data upon which business decisions are being made cannot be assured.

Availability of the Data

Finally, the appropriate access control settings can contribute to the availability—or not—of the organization's data. If, from outside of the protection of application logic, the default access control setting or the users' permissions to the database files allows modification of data, removal of records, or the clearing or deletion of files, the data may not be available for use. Take, for example, an analyst that downloads data to spreadsheets. One day they accidently press the wrong icon and data from last month's analysis is uploaded to the production database. The production database is now out-of-date and has to be restored from back-up and recent transactions re-entered. Or the root directory is shared and users are automatically re-connected to the share. They open Windows Explorer and see Libraries that shouldn't be on their PC. Not realizing that they are acting on Libraries on the system rather than their individual PC, they drag and drop production libraries to the Trash. Think these are made-up examples? Think again.

Actions such as these are unintentional and non-malicious. But regardless of motive, the result is an outage and a very preventable one at that. When users are given only the permission they need to perform their job functions—outages such as these are prevented.

Multiple Layers of Defense

One you've determined the value of the data to your organization you may choose to apply multiple layers of security. For example, you may have data that does not fall under any formal compliance requirements. However, it is so valuable to your organization or the cost to your organization would be so great if it were lost, that you decide to not only set the permissions on the database to be 'deny by default'

CMI (Chouinard & Myhre, Inc.)
655 Redwood Hwy, Ste. 102
Mill Valley, CA 94941
415.480.3636
www.cm-inc.com

you also encrypt the information. Or, perhaps you decide to add biometric authentication so that only certain users can perform certain functions within the application.

While some regulations such as PCI DSS do require multiple layers of defense, most do not. Therefore, the number of layers implemented will be determined by your organization's requirements. The more risk-adverse your organization is, the more layers of defense you'll apply to ensure the data is protected.

Summary

If the data falls under regulatory compliance requirements you have some idea of how much security is enough. But whether the compliance requirements are enough will be up to your organization to determine. Of course, if the data does not fall under regulatory requirements the value of the data to your organization will answer the question—how much is enough. Regardless, numerous benefits are realized by answering the question, "How much security is enough?" and securing an organization's data appropriately. Here are just a few:

Compliance With Regulatory Requirements: Data that is secured according to the laws and regulations under which is falls will not suffer from the potential fines, audit findings, legal issues, and negative publicity associated with non-compliance.

Integrity Of Data: Properly secured data can be relied upon to be accurate. That is, it can be assured that only those roles that should be allowed to modify data are and all others are denied or are read-only.

Privacy And Confidentiality Of Data: Some data should not only be updated by selected roles but some data should only be viewed by selected roles. If data is set to be deny-by-default, the confidentiality and privacy of the data can be assured.

Availability Of Data: If the access control settings of data allows any user to modify or worse, delete, records or files, the availability of the data cannot be assured.

Carol Woodbury is President and Co-founder of SkyView Partners, Inc. and is certified in Risk and Information Systems Control. Carol has over 20 years experience in the area of security and is an award-winning speaker and writer. Her latest book, **IBM i Security Administration and Compliance** *is now available.*

CMI (Chouinard & Myhre, Inc.)
655 Redwood Hwy, Ste. 102
Mill Valley, CA 94941
415.480.3636
www.cm-inc.com

iStatus Check — By Kris Neely, CMI's Chief Technology Officer

Data — today, firms worldwide are drowning in data. Yet I meet client after client who have not sat down and determined a data management strategy (on paper, that is. A data management 'strategy' that isn't on paper isn't a strategy: it's an idea.)

For those who have written a data management strategy, even fewer have integrated their data security and data management strategies. Typically, although not in all cases, these two strategies live apart, and data security is often bolted-on to data management. Or vice versa.

Net result: organizational risk, data vulnerability, and an open invitation to increased IT and organizational costs.

This is particularly ironic considering there are more data management and data security tools, packages, and documented best practices than ever before. These topics are not 'bleeding-edge' with only a few mountain top gurus who really know the inside scoop. So why the gap between what should be and what is in data management and security?

Sadly, I think it's largely a lack of management buy-in. If executive (CXX-level) management realized the real risk to an organization … the real costs of remediation … the potential costs (money, time, people, etc) involved, I think we'd see a different picture. Hope — is a bad plan for anything in IT, but considering the cautions flags highlighted in this White Paper, it's particularly woeful in data management & security.

When was the last time you reviewed your firm's data management & data security strategies, tactics, tools, operations, and documentation?

Be well.
Kris
CTO
Chouinard & Myhre, Inc.

CMI (Chouinard & Myhre, Inc.)
655 Redwood Hwy, Ste. 102
Mill Valley, CA 94941
415.480.3636
www.cm-inc.com

Reality Check -- CFO Endorsement for CMI White Paper on Data Security

I find that the approach to data protection is often analogous to buying insurance. The rule for buying insurance is generally to only insure that which you cannot afford to lose, or which you are required to have. But data protection is more subtle than this and any company that does not take a considered approach is likely wasting resources or exposing themselves to unnecessary risk.

My background is in the entertainment industry, and data security was always essential for our clients especially as the industry digitized, an issue highlighted when the movie Wolverine was stolen weeks before release. It made the industry suddenly realize that the world had changed and that new risks to the security of their IP had arisen.

The movie industry responded with new processes, contracts and security reviews. Obviously this was an important part of our responsibilities to our clients, but our own data, our secret sauce, also had to be protected without getting in the way of the essential collaboration that created our competitive advantage in the first place. Having our employees suddenly jump through new hoops or have to wait for the IT department to give an artist access to a certain file or folder was not a realistic option.

In terms of your data, it is important to have an approach to security that is part of the DNA of the company, meaning it fits with the goals and objectives, but is not overly burdensome and is well understood and appreciated by the employees. Security needs to be part of the day to day process and mindset of the organization, not just a system. If this is not the case, your company can be exposed to risk or inefficiency without your knowledge. Looking at this subject once a year is not a solution and does not breed the sort of behavior you need.

The world of IT systems is always rapidly changing and this has an impact on your security procedures. Consider the recent advances in adoption of smartphones – how much company data, such as confidential e-mails, is now stored locally on those devices? You can choose to prevent their use, but does that result in a loss of productivity? This example is even more relevant if your company is moving to the cloud.

In my experience, this is an area where relying on your head of IT or your CTO alone is often not sufficient. Specialist experience and knowledge of current macro risks and solutions is required as is a review of the overall processes that are required to make the security systems as effective and low-impact as possible.

Ensuring you have enough security, but not too much, is a tricky balance, but the answer to the question lies in truly understanding the risks and the burden of compliance and then making sure that this is becomes part of the DNA of your company.

Kevin Weston, Former CFO Digital Domain Productions, VP Finance and Operations of LucasArts and CFO/SVP Finance and Operations at Eidos Interactive Inc.

CMI (Chouinard & Myhre, Inc.)
655 Redwood Hwy, Ste. 102
Mill Valley, CA 94941
415.480.3636
www.cm-inc.com