How to Sell Backup to Your CFO

(Going Beyond the Insurance Metaphor to Create a Value Proposition for Data Protection)

UNITRENDS

7 Technology Circle
Suite 100
Columbia, SC 29203

Phone: 866.359.5411
E-Mail: sales@unitrends.com
URL: www.unitrends.com

How to Sell Backup to Your CFO

A CEO throwing a party takes his executives on a tour of his opulent mansion. In the back of the property, the CEO has the largest swimming pool any of them has ever seen. The huge pool, however, is filled with hungry alligators. The CEO says to his executives "I think an executive should be measured by courage. Courage is what made me CEO. So this is my challenge to each of you: if anyone has enough courage to dive into the pool, swim through those alligators, and make it to the other side, I will give that person anything they desire. My job, my money, my house, anything!"

Everyone laughs at the outrageous offer and proceeds to follow the CEO on the tour of the estate. Suddenly, they hear a loud splash. Everyone turns around and sees the CFO in the pool, swimming for his life. He dodges the alligators left and right and makes it to the edge of the pool with seconds to spare. He pulls himself out just as a huge alligator snaps at his shoes.

The flabbergasted CEO approaches the CFO and says, "You are amazing. I've never seen anything like it in my life. You are brave beyond measure and anything I own is yours. Tell me what I can do for you." The CFO, panting for breath, looks up and says, "You can tell me who the hell pushed me in the pool!!"

Don't be the one who pushed.

A CFO is a corporate officer primarily responsible for managing the financial risks of the corporation. Secondary responsibilities are financial planning and record keeping as well as financial reporting to senior management as well as the board of directors.

Given that job description, you would think that "selling backup" to a CFO would be the easiest thing in the world. You'd be wrong. Some CFOs intuitively grasp the linkage of data protection to the limitation of financial risk to a company. Other CFOs tend to focus on minimizing costs and see data protection as an unnecessary expense from an IT department that is always wanting to spend more money on all forms of information technology.

Traditionally the way that IT leaders have tended to "sell backup" is by using an insurance metaphor. Data protection, like various forms of insurance, is an expense intended to protect the corporation against foreseen and unforeseen events that could endanger the corporation. More formally, insurance is a form of financial risk management used to hedge against the risk of a contingent, uncertain loss. Note that term "financial risk management"; it's that concept that makes the insurance metaphor so appealing because it aligns so neatly with the primary responsibility of the CFO.

In this document we're first going to explore the use of the insurance metaphor in terms of its most fundamental element: the broad consequences of data loss. We'll also discuss industry and regulatory consequences of data loss.

After that we'll go beyond the insurance metaphor and present three additional mechanisms for selling data protection to the CFO

- Optimizing capital expenditure
- Optimizing operational expenditure
- Optimizing productivity through RPO and RTO

Using the Insurance Metaphor

What Are the Broad Consequences of Data Loss?

The consequences of data loss are dire; here is a sampling of just a few statistics related to the impact of data loss on business:

- 93% of companies that lost their data center for 10 days or more due to a disaster, filed for bankruptcy within one year of the disaster. 50% of businesses that found themselves without data management for this same time period filed for bankruptcy immediately. (National Archives & Records Administration in Washington)

- 94% of companies suffering from a catastrophic data loss do not survive - 43% never reopen and 51% close within two years. (University of Texas)

- 30% of all businesses that have a major fire go out of business within a year and 70% fail within five years. (Home Office Computing Magazine)

- 77% of those companies who do test their tape backups found back-up failures. (Boston Computing Network, Data Loss Statistics)

- 7 out of 10 small firms that experience a major data loss go out of business within a year. (DTI/Price waterhouse Coopers)

- 96% of all business workstations are not being backed up. (Contingency Planning and Strategic Research Corporation)

- 50% of all tape backups fail to restore. (Gartner)

- 25% of all PC users suffer from data loss each year (Gartner)

What Are the Industry Consequences of Data Loss?

Data loss costs will tend to vary by industry because the dependence upon technology and data is correlated to industry. Of course, there's a wide variance within an industry by a number of other factors such as company size, corporate psycho graphics in terms of technology adoption, and other factors.

There is no available breakdown of cost on an industry basis; however, in 2000 the Meta Group surveyed various industries and computed the cost of downtime. This information is depicted in the table below.

Industry	Hourly Downtime Cost
Brokerage Operations	$6,450,000
Energy	$2,817,846
Credit Card Sales Authorizations	$2,600,000
Telecommunications	$2,066,245
Manufacturing	$1,610,654
Financial Institutions	$1,495,134
Information Technology	$1,344,461
Insurance	$1,202,444
Retail	$1,107,274
Pharmaceuticals	$1,082,252
Banking	$996,802
Food/Beverage Processing	$804,192
Consumer Products	$785,719
Chemicals	$704,101
Transportation	$668,586
Utilities	$643,250
Health care	$636,030
Metals/Natural Resources	$580,588
Professional Services	$532,510
Electronics	$477,366
Construction and Engineering	$389,601
Media	$340,432
Hospitality and Travel	$330,654
Pay-Per-View TV	$150,000

Industry	Hourly Downtime Cost
Home Shopping TV	$113,000
Catalog Sales	$90,000
Airline Reservations	$90,000
Tele-Ticket Sales	$69,000
Package Shipping	$28,000
ATM Fees	$14,500

Beyond the immediate financial impact of data loss, other consequences include a loss of customer confidence, corporate liability, and the loss of current and future business.

What Are the Regulatory Consequences of Data Loss?

Regulatory compliance describes the goal that corporations or public agencies conform and comply with relevant laws and regulations. CFOs care about regulatory compliance because the consequences of not being able to prove compliance - these tend to range from corporate fines to in the most egregious cases involving loss of personal freedom.

Regulatory compliance tends to vary by locale; the more prominent regulations are specified in the sections below.

SOX (Sarbanes-Oxley or Sarbox)

SOX is a set of regulations associated with all public companies in the United States. The applicable sections of SOX as it pertains to data protection include

Section 103: Auditing, Quality Control, And Independence Standards And Rules
The Board shall: (1) register public accounting firms; (2) establish, or adopt, by rule, "auditing, quality control, ethics, independence, and other standards relating to the preparation of audit reports for issuers;" "The Board requires registered public accounting firms to "prepare, and maintain for a period of not less than seven years, audit work papers, and other information related to any audit report, in sufficient detail to support the conclusions reached in such report."

Section 104: Inspections of Registered Public Accounting Firms
Quality inspections must be conducted annually for firms auditing more than 100 issues per year, or every 3 years for all other firms. The SEC or the Board may order impromptu inspections of any firm at any time.

Section 105(d): Investigations And Disciplinary Proceedings; Reporting of Sanctions
All documents prepared or received by the Board are regarded "confidential and privileged as an evidentiary matter (and shall not be subject to civil discovery or other legal process) in any proceeding in any Federal or State court or administrative agency, ...unless and until presented in connection with a public proceeding or [otherwise] released" in connection with a disciplinary action.

Title VIII: Corporate and Criminal Fraud Accountability Act of 2002
"Knowingly" destroying or creating documents to "impede, obstruct or influence" any federal investigation, whether it exists or is contemplated, is a felony.

Section 802: Document Alteration or Destruction
This section instructs auditors to maintain "all audit or review work papers" for five years from the end of the fiscal period during which the audit or review was concluded. It also directs the Securities and Exchange Commission (SEC) to disseminate, within 180 days, any necessary rules and regulations relating to the retention of relevant records from an audit or review. This section makes it unlawful knowingly and willfully to violate these new provisions -- including any rules and regulations disseminated by the SEC -- and imposes fines, a maximum term of 10 years' imprisonment or both.

Section 1102: Tampering With a Record or Otherwise Impeding an Official Proceeding
This section forbids knowingly altering, destroying, mutilating, or concealing any document with the intent to impair the object's integrity or availability for use in an official proceeding or to otherwise obstruct, influence or impede any official proceeding.

FACTA (Fair and Accurate Credit Transactions Act)

FACTA is a United States federal law that allows consumers to request and obtain a free credit report once every twelve months as well as provisions to reduce identity theft. With respect to data protection, FACTA requires secure disposal of consumer information.

The requirement regarding secure disposal of consumer information means that the secure and timely disposal of applicable backup information must be able to be performed.

GLBA (Gramm-Leach-Bliley Act)

GLBA is a comprehensive United States law requiring all institutions associated with financial transactions to protect the security, integrity, and confidentiality of consumer information. GLBA affects an extremely wide range of organizations including banking institutions, insurance companies, securities firms, mortgage brokers, security firms, financial advisors, real estate brokers, collection agencies, tax preparers, and credit card companies.

The most pertinent GLBA requirements with respect to data protection are specified below (these are from the section of the law known as the "Safeguard Rule."

Insure the security and confidentiality of customer records and information.

To protect against any anticipated threats or hazards to the security or integrity of such records.

To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

FISMA (Federal Information Security Management Act)

FISMA is a United States act that mandates security programs for all organizations which possess or use federal information systems on behalf of a federal agency. The act holds senior management accountable for ensuring the timely implementation of security measures. By viewing IT security as a life cycle process, FISMA integrates security with overall IT management and maintenance processes.

Government agencies will soon be required to meet the standards published in the Minimum Security Requirements for Federal Information and Information Systems document, also referred to as FIPS 200. These standards, currently published by the National Institute of Standards and Technology as special publication 800-53, further detail the specific implementation requirements to heighten security within government information systems.

HIPAA (Health Insurance Portability and Accountability Act)

HIPAA is a set of regulations associated with the United States health care industry. The major applicable requirements associated with HIPPA are as follows:

Electronic personal health information (ePHI) must be protected against any reasonably anticipated threats or hazards.

Access to ePHI must be protected against any reasonably anticipated uses or disclosures that are not permitted or required by the Privacy Rule.

Maintenance of record of access authorizations.

If the data is processed through a third party, entities are required to enter into a chain of trust partner agreement.

ITIL (IT Infrastructure Library)

ITIL is a series of books developed by OGC (Office of Government Commerce, a part of the United Kingdom government) in response to the growing dependency on IT. The intent if ITIL is the encapsulation of a set of best practices for IT service management.

DPA (Data Protection Act 1998)

DPA is a United Kingdom Act of Parliament which defines the law with respect to data and the processing of that data on identifiable living people. It was enacted to bring UK law into line with the European Directive of 1995 which required Member States to protect people's fundamental rights and freedoms and in particular their right to privacy with respect to the processing of personal data.

The summary of the key principles of DPA is given below:[1]

Data may only be used for the specific purposes for which it was collected.

Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the information (for example, the prevention or detection of crime). It is an offense for Other Parties to obtain this personal data without authorization.

Individuals have a right of access to the information held about them, subject to certain exceptions (for example, information held for the prevention or detection of crime).

Personal information may be kept for no longer than is necessary and must be kept up to date.

Personal information may not be sent outside the European Economic Area unless the individual whom it is about has consented or adequate protection is in place, for example by the use of a prescribed form of contract to govern the transmission of the data.

Subject to some exceptions for organizations that only do very simple processing, and for domestic use, all entities that process personal information must register with the Information Commissioner's Office.

Entities holding personal information are required to have adequate security measures in place. Those include technical measures (such as firewalls) and organizational measures (such as staff training).

Subjects have the right to have factually incorrect information corrected (note: this does not extend to matters of opinion)

Going Beyond the Insurance Metaphor: Optimization

Like all metaphors, the insurance metaphor for data protection breaks down when analyzed in more detail. Insurance is at its core a risk transfer mechanism in which a company transfers risk in exchange for a financial payment. Data protection is at its core a key characteristic of a corporation's information technology strategy. As such, what must be sought is not just insurance but optimization. To a CFO, optimization fundamentally means higher productivity; to wit, an increase in projected revenue with the lowest projected possible expense.

1 Source: Wikipedia

In this section, we'll discuss three fundamental methods of achieving higher productivity with respect to the data protection strategy of a company:

- Achieving higher productivity by optimizing capital expenditure.
- Achieving higher productivity by optimizing operational expenditure.
- Achieving higher productivity by optimizing RPO (Recovery Point Objective) and RTO (Recovery Time Objective) for the needs of your business.

Every CFO has a strong focus on optimizing capital expenditure - after all, capital is money. Depending upon the industry, staffing can be as much as 80% or more of the on-going expense rate of a company; operational expenditure is thus a critical factor for a CFO seeking to increase the productivity of a corporation. As we noted previously, capital is money - and since operations is time and time is money then optimizing capital expenditure and operational expenditure is critical.

The third fundamental method of achieving higher productivity involves optimizing the RPO and RTO associated with data protection. The RPO and RTO together essentially define the amount of time that will be spent recreating data. This will be discussed in detail in the last section of this chapter.

Optimizing Capital Expenditure

Optimizing capex (capital expenditure) is the foundation of optimizing for productivity. With the advent and growing penetration of commodity x86-based virtualization, there has been a strong focus within IT with respect to decreasing capex over the last few years.

There are several ways that IT leaders can convince CFOs that they are focused on optimizing capital expenditure. One way is to not buy more backup capacity than is needed; in other words, don't buy ahead of your backup capacity needs. Select a backup technology that is inherently scalable such that multiple backup systems can be monitored and managed via a single pane of glass. If you don't do this, then what you end up doing is spending a lot of money on backup capacity - either using dedicated deduplication devices or by buying raw storage - and the facts are that storage pricing has been and is continuing to demonstrate a rapidly decreasing price per effective terabyte..

This is really just common sense. You don't buy too much of anything, whether it is backup capacity or toilet tissue, when you know that the price is going to be falling in the future.

Focus on your overall backup spending in terms of your spend on a per terabyte basis. There's a lot of different deduplication technologies out there; make sure that you're not spending more on a per terabyte basis for deduplication unless there's no other way to achieve your retention needs.

Another way to optimize capital expenditure is to make sure that you keep your primary storage spending as lean as possible. This doesn't mean not to buy centralized storage, such as NAS or SAN, but it does mean that you don't want to rely only upon centralized storage as your only storage vehicles. And while techniques such as snapshots can be used very effectively to optimize your data protection strategy, don't lock into expensive solutions such as SAN replication that require a doubling (or more) of your storage budget without giving you the type of data protection flexibility you'll need.

Optimizing Operational Expenditure

It is the nature of every technology industry to tout its features and promote the attributes of its offerings. The data protection segment is no different; there are many companies discussing in exhausting detail the latest feature/functionality that has been released. George Crump at Storage-Switzerland has identified the three top areas with respect to data protection that cause the most wasted time:

- Making sure that all backups are completed.
- Squeezing out that last bit of performance.
- Dealing with the agile data center.

The first thing that's needed to make sure backups are completed is an integrated management and monitoring system designed for simple single-pane of glass dashboard operation so that you can tell the status of your backups and your vaulting (disaster recovery) operations at a glance. You want to make sure that you either use a single integrated and federated system or you want to make sure you can integrated disparate point solutions into a single dashboard system. Of course, the more point solutions you have the more time you're going to spend writing scripts and integrating them; so you want to minimize the number of point solutions whenever possible.

Squeezing out that last bit of performance from a data protection solution is incredibly problematic. Quite often there is a direct trade-off here between capital expenditure and operational expenditure. Keep your options open by using a scalable system which allows you to attach to any network segment but still allows you to monitor and manage from that single pane of glass.

The concept of the agile data center sounds good until you realize that this means that you will be constantly adapting and responding your data protection to that agility. Make sure that you have a flexible data protection system that can respond to that agility via not only scalability but through the flexibility of working in a heterogeneous environment with respect to not only compute platforms, operating systems, and applications but also heterogeneous storage as well.

Optimizing Productivity through RPO and RTO

The first two optimization techniques discussed centered entirely around reducing expenditure - both capital expenditure and operational expenditure. In essence, these first two techniques are focused on increasing productivity through reducing on-going cost.

The technique discussed in this section is focused on increasing productivity through reducing the operational cost when a data loss event actually occurs.

First, a few definitions:

- RPO: The amount of work that can be lost and will need to be redone in the case of data loss.
- RTO: The amount of time it will take before employees can start working after a data loss event.
- Productivity Loss: RPO + RTO
- Cost: Productivity Loss x Total Hourly Rate of Effected Employees

Thus the answer here is to minimize RPO and RTO, right? Not so fast. What you want to do when you're making a proposal to your CFO is that you've shown that you've thought through the problem and that the solution you propose will deliver the most bang for the buck.

The first thing you need to think about is how you'll recover your system, not just your data. Your RTO will be dramatically impacted if you don't have some form of bare metal recovery. Bare metal recovery simply means that you're able to restore your systems and not just individual pieces of data. In particularly, look for what is called dissimilar bare metal recovery on both a physical-to-physical (P2P) and on a virtual-to-physical and physical to virtual (V2P and P2V, respectively.)

In terms of your RPO, you want to make sure you balance your desired RPO against your desired retention. Also make sure that your data protection solution can flexibly support technologies such as SAN snapshots so that you can achieve protection against logical failure while you also have protection against physical failure by moving sufficient data from your primary storage device.

Understand whether you have different RPO needs for different types of data. Typically structured data, such as databases and e-mail, require a faster RPO than unstructured data (file systems.) In addition, different protected clients may have different RPOs as well. The ability to easily define different RPOs for different types of data and for different systems is important.

One thing that many people take for granted is the fact that your RPO and RTO should be measured against all of your IT assets distributed throughout your company and not just those that are within your data center. What is the RPO and RTO for the notebooks, workstations, and PCs within your environment? It's wonderful to talk about lowering your RPO and RTO, but if you haven't included all of the IT assets then you're just kidding yourself in terms of what your overall protection levels are.

Summary

There's no silver bullet in terms of convincing your CFO that data protection is vital to reduce the financial risk to your company. However, if you use the insurance metaphor, taking into account your industry-specific needs and your regulatory requirements, and then extend the insurance metaphor to show specifically the increased productivity possible via optimization, then you will create a bridge between you and your CFO in terms of a shared understanding of risk and reward. Most importantly, show your CFO that you take the financial side of this as seriously as he or she does and ensure that you get the most "bang for the buck" in terms of your solution.

About Unitrends

Unitrends offers a family of affordable, all-in-one on-premise backup appliances that support virtual and physical system backup and disaster recovery via disk-based archiving as well as electronic vaulting to private- and public-clouds. Unitrends is customer-obsessed, not technology-obsessed, and is focused on enabling its customers to focus on their business rather than on backup.

For more information, please visit www.unitrends.com or email us at sales@unitrends.com.

7 Technology Circle, Suite 100
Columbia, SC 29203

Phone: 866.359.5411
E-Mail: sales@unitrends.com
URL: www.unitrends.com