How to Sell Backup to Your CFO

Use the Insurance Metaphor (and More)

To Demonstrate the Value of Data Protection

UNITRENDS

www.unitrends.com

How to Sell Backup to Your CFO

A CEO is throwing a party. He takes his executives on a tour of his opulent mansion. In the back of the property, the CEO has a huge swimming pool. The pool, however, is filled with hungry alligators. Noting their alarm, the CEO says to his executives "I think an executive should be measured by courage. Courage is what made me the CEO. This is my challenge to each one of you: anyone who has enough courage to dive into the pool, swim through those alligators, and make it to the other side, will have anything they desire—including my job, my money, my house, anything!"

Everyone laughs at the outrageous offer and continues 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, pulling himself out as an alligator snaps at his shoes. The flabbergasted CEO approaches the CFO and says, "You are amazing. I've never seen anything like this in my life. You are brave beyond measure. 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!

The CFO is a corporate officer whose primary responsibility is managing the financial risks of the corporation. Secondary responsibilities include financial planning and record keeping as well as financial reporting to senior management and the board of directors.

Given that job description, you would think "selling backup" to a CFO would be easy. Wrong. The importance of backup is often overlooked. Yet consider the consequences if you have an outage and no backup—you are exposed. It is time-consuming to recreate lost work. Or if you have an audit and no backup, you are at risk. And in many instances monetary fines are imposed as well.

Some CFOs intuitively grasp the relationship between data protection and financial risk to a company so they approve of backup expenditures. Yet other CFOs, focused on minimizing costs, believe that existing backup practices are adequate and additional data protection is an unnecessary expense from the IT department. Do these CFOs predominate? Maybe.

As a result IT managers have attempted to "sell backup" using an insurance metaphor. Data protection, like other forms of insurance, is an expense intended to protect the corporation in the event of foreseen or unforeseen events that put the corporation at financial risk. In other words, insurance is a type of financial risk management used to hedge against the possibility of a contingent, uncertain loss. Note the term "financial risk management." It is a concept that makes the insurance metaphor appealing because it aligns with the primary responsibility of the CFO.

In this document we have a few objectives. First we aim to help IT managers cost justify data protection using the insurance metaphor, applied against the broad consequences of data loss. This approach is associated with implied loss and uses statistics to infer possibilities. Next we review a simple method to calculate the downtime cost for an individual organization; we get specific so you can see where your company falls in the range of industry statistics.

After the insurance metaphor, we discuss optimization as it impacts costs. We show how to cost-justify data protection to the CFO using three key financial concepts noted:

- Optimization of capital expenditure.
- Optimization of operational expenditure.
- Optimization of productivity, applying recovery metrics RPO and RTO.

Finally, we expand the definition of data protection to include retention and recovery as they deserve extra consideration. We highlight recent surveys on the topic of business continuity and disaster recovery planning to better understand problems we identified earlier. Also we review regulatory compliance because it drives backup, retention, and retrieval needs in some industries. Note that not all regulatory compliance carries financial penalties but most do; there is a financial consequence to non-compliance. We close with a discussion of cloud storage retention, disaster recovery as a service, and disaster recovery testing to be sure we cover all the bases.

In conclusion, the goal of this document is to give you, the IT manager, the tools to 'sell backup' and data protection to your CFO. We want to be as comprehensive as possible to make you successful in that endeavor.

Using the Insurance Metaphor

What Are the Broad Consequences of Data Loss?

The consequences of data loss can be dire. Regardless of a natural or man-made catastrophe, here are some current statistics assessing the impact of data loss on business:

Aberdeen Group surveyed IT managers in May 2013 for "IT Business Preparedness: A combination of Business Continuity and Disaster Recovery." All organizations, independent of size, suffer significant financial losses for every second, minute or hour of disruption. Aberdeen calculated the average cost-per-hour of downtime for all respondents and reported:

- Average downtime cost-per-hour was over $163,000.
- Small companies lost over $8,000 per hour.
- Medium size firms lost over $215,000 per hour.
- Large organizations reported losses of over $600,000 per hour.

Timico, a UK communications service provider, surveyed IT managers in March 2015 and found:

- Over 70 percent (70%) of IT managers have never worked out the cost of the resulting downtime despite outages.
- Despite the risks, a minority of respondents admitted to never backing up their data.

Vanson Bourne surveyed 3300 IT decision makers from mid-size to enterprise-class businesses in 24 countries during 2014 for EMC and discovered:

- Data loss and downtime cost enterprises more than $1.7 trillion in the last twelve months.
- The number of data loss incidents is decreasing overall but the volume of data lost during an incident is growing.
- Seventy-one percent (71%) of organizations are not fully confident in their ability to recover after a disruption.
- The average business experienced more than three working days (25 hours) of unexpected downtime in the last 12 months.
- Other commercial consequences of disruptions were loss of revenue and delays to product development.
- Businesses using three or more vendors to supply data protection solutions lost three times as much data as those who unified their data protection strategy around a single vendor. They were also likely to spend an average of $3 million more on their data protection infrastructure compared to those with just one solution.

Dynamic Markets surveyed 210 IT professionals in large organizations in the US, Canada and UK during 2014 for Avaya and noted:

- Eighty-two percent (82%) of respondents experienced network downtime caused by IT personnel making errors when configuring changes to the core of the network.
- Eighty percent (80%) of companies experienced downtime and lost revenue, averaging $140,003 per incident. The financial sector lost more—an average of $540,358 per incident.
- One in five companies fired an IT employee when a network downtime incident occurred. One in three companies in the natural resources, utilities & telecoms sector sacked IT staff due to downtime caused by change errors.

Tech Validate conducted a survey of 340 IT end users all over the globe in March/April 2015 for Imation and discovered:

- Three of the four most common file types in organizations' data centers are office productivity documents, images and rich media (all unstructured data sets). This data is considered to be high-value and contributes to most of the data growth.
- Seventy percent (70%) of organizations have corporate policies governing where high-value data should be stored.
- Fifty-five percent (55%) of these respondents said they are "unsure" or "not confident at all" that their organization's files are being backed up.
- Twenty-five percent (25%) of respondents said they do not have any barriers to deploying proactive file security solution.
- The majority of high-value data is not confidently protected.

What is the Cost of your Lost Data?

Data loss cost varies by industry as well as by company size. Deployed technology (physical-only versus physical-virtualized server on-site; client location including network; cloud versus non-cloud, remote retention media off-site; etc.) and data managed creates more variability. While there is no reliable breakdown of downtime cost by industry, some analyst firms have created downtime calculators to proxy downtime cost.

Find a calculator you like and collect the necessary data to determine the cost of downtime (see Appendix A for an example). Is the downtime cost less/equivalent/more than the cost of a data protection solution? Based on one event, If this cost is less or equivalent, invest in a data protection solution. You will save money given the probability of an outage in the future.

Remember beyond the immediate financial impact of data loss, other consequences include a loss of customer confidence, corporate liability and the potential loss of current and future business. These events have a cost as well.

Going Beyond the Insurance Metaphor

Multiple Approaches to Address Optimization

Like many metaphors, this one for data protection can break down if analyzed in more detail. Fundamentally insurance is a risk transfer mechanism; by definition the act of protection against loss, arising in specified contingencies, in consideration of a payment proportionate to the risk involved. Ultimately we seek more, we seek risk mitigation. As data protection is a key component of a corporation's information technology

strategy we want to lower the risk—and cost associated with it. Consequently, instead of insurance, we need to optimize cost. To a CFO, this optimization can be translated into higher productivity and profit (increase in projected revenue with the lowest possible expense).

In this section, we discuss three methods to optimize costs and achieve higher productivity with respect to the data protection strategy of a company:

- Optimization of capital expenditure.
- Optimization of operational expenditure.
- Optimization of productivity, applying recovery metrics RPO and RTO.

Capital expenditure (CAPEX) are funds used to acquire or upgrade physical assets. Every CFO is focused on the optimization of capital expenditure as budgets are tight if not fixed. It makes sense to get the most value possible for the money too.

Operation expenditure (OPEX) are costs incurred in normal business operations. Labor cost is often a large portion of OPEX; depending upon the industry, staffing can be as much as 80% or more of OPEX. OPEX is a critical component of the optimization equation.

The third way to achieve higher productivity applies to specific instances of CAPEX and OPEX associated with IT strategy. For example, IT service delivery, one element of IT strategy and the company's overall budget, establishes the foundation for business operations such as sales that relies on CRM or finance that needs access to ERP systems. Multi-faceted, IT strategy embraces all risk and hence data protection. Cost effective data protection is measured using the recovery point objective (RPO) and recovery time objective (RTO). The RPO and RTO together define the amount of time that will be spent to recreate data in the event of an outage and disruption in business operations.

Optimizing Capital Expenditure

Optimization of your capital expenditure is critical to achievement of higher productivity. No surprise that with the advent and penetration of commodity x86-based servers and virtualization, there has been a renewed focus to decrease CAPEX attributed to IT over the last few years.

In response, there are several ways IT managers can convince CFOs that they are also focused on optimization of capital expenditure. For data protection, one way is to only buy what you need today; in other words, don't buy ahead of your backup capacity needs. Or look at hybrid cloud—with extensions to third party cloud—to provide flexible capacity for additional retention. In any case, do select a backup technology that is inherently scalable—and one that monitors and manages multiple backup systems via a single pane of glass. If you do not, you could spend a lot of money on additional backup capacity in the form of raw storage, regardless if the price of storage has been and continues to decrease.

It is common sense: don't buy too much of anything—including backup capacity—when the price is falling.

Instead you might look at a backup solution in terms of spend per terabyte (total cost for the solution divided by the terabytes of storage offered by solution). Today most backup solutions embed various deduplication technologies in their solutions. There are many different types (source, server, appliance-based deduplication). Just be sure you are not spending more per terabyte unless there is no other way to meet your needs.

Another way to optimize capital expenditure is to make primary storage spending as lean as possible. There are many solutions on the market to meet your needs—centralized storage, network attached storage (NAS), storage area networks (SAN), cloud storage. Each solution offers different management techniques

(e.g. snapshots, mirroring, clustering) to optimize your storage and support your IT strategy. Note that cloud storage offers an additional benefit—no on-premise equipment to maintain. Remember, however, a heterogeneous IT environment means there are many disparate physical and virtual systems to manage. Think about this reality when you select your data protection solution because you need to integrate all pieces to support IT services delivery and optimal really does mean ALL.

Optimizing Operations Expenditure

Many vendors in the technology industry tout features to promote product offerings. Data protection vendors are no different; many companies push their latest released features and forget the benefits. Benefits should include saving time in addition to lower/lowest cost. Saving time translates to saving labor and labor is an operational expense.

On the topic of saving time, George Crump of Storage-Switzerland identified three areas that cause wasted time with respect to data protection solutions:

- Incomplete backups.
- Performance that is not optimized.
- Inflexible solutions.

We agree. Make sure your backups are complete. Use a solution that offers integrated management and monitoring with a simple single-pane of glass dashboard so you can determine the status of your backups and vaulting (disaster recovery) operations at a glance. Make sure you use either a single integrated and federated system—or one that integrates different point solutions on a single dashboard system. And remember, more point solutions mean additional time will be spent on writing scripts to integrate them. Minimize the number of point solutions whenever possible for optimal performance.

Squeeze the last bit of performance from your data protection solution. Idle time is money. Note that quite often there is a trade-off between capital expenditure and operational expenditure. You can create options for yourself by using a scalable system that allows you to attach to any network segment from a single pane of glass.

And the agile data center has arrived. It sounds like a good idea until you realize that 'agile' means you will be constantly adapting the data center and the corresponding data protection plan. Make sure that you have a flexible data protection system to respond to agility with scalability and flexibility. Operations in a heterogeneous IT environment mean not only managing different compute platforms, operating systems and applications but different storage systems as well.

Optimizing Productivity: The Recovery Point Objective (RPO) and Recovery Time Objective (RTO)

The first two optimization methods discussed include capital expenditure and operational expenditure. We provide examples as to how these concepts relate to backup and data protection. Straightforward financial concepts.

The next method discussed is tangential because it draws on both capital and operations expenditures to attain optimization goals. Deployed correctly, data protection should increase productivity through a reduction in operations cost when a data loss event actually occurs. And if you select a cost effective data protection solution it will mean lower capital expense.

Let's review a few definitions and related points:

- RPO: Amount of work lost (time between data backups and the amount of data that could be lost in between backups). This work will need to be recreated in the event of data loss.
- RTO: Total amount of time it will take before employees can effectively use IT assets after a data loss event. Or the target time you set for the recovery of your IT and business activities after a disaster has struck.
- The major difference between these two metrics is their purpose. The RTO is larger in scale and looks at the whole business and the systems involved. RPO focuses only on data and your company's overall resilience to the loss of it.
- Creating a tighter RPO and RTO means you will spend more money on your infrastructure (CAPEX).

While it seems like the goal of your backup strategy should be to minimize RPO and RTO, that decision might be pre-mature. When you make that proposal to your CFO, illustrate that you have thought through all angles of data protection and then the solution you propose will deliver the biggest bang for the buck. Some ideas to consider:

First, think about how you will recover your system not just your data. Your RTO will be impacted if you don't have some form of bare metal recovery. Bare metal recovery means that you can restore your systems to their initial state and not just individual pieces of data. In particular, look for what is called dissimilar bare metal recovery on both the physical-to-physical (P2P) hardware as well as the virtual-to-physical and physical to virtual (V2P and P2V, respectively) hardware.

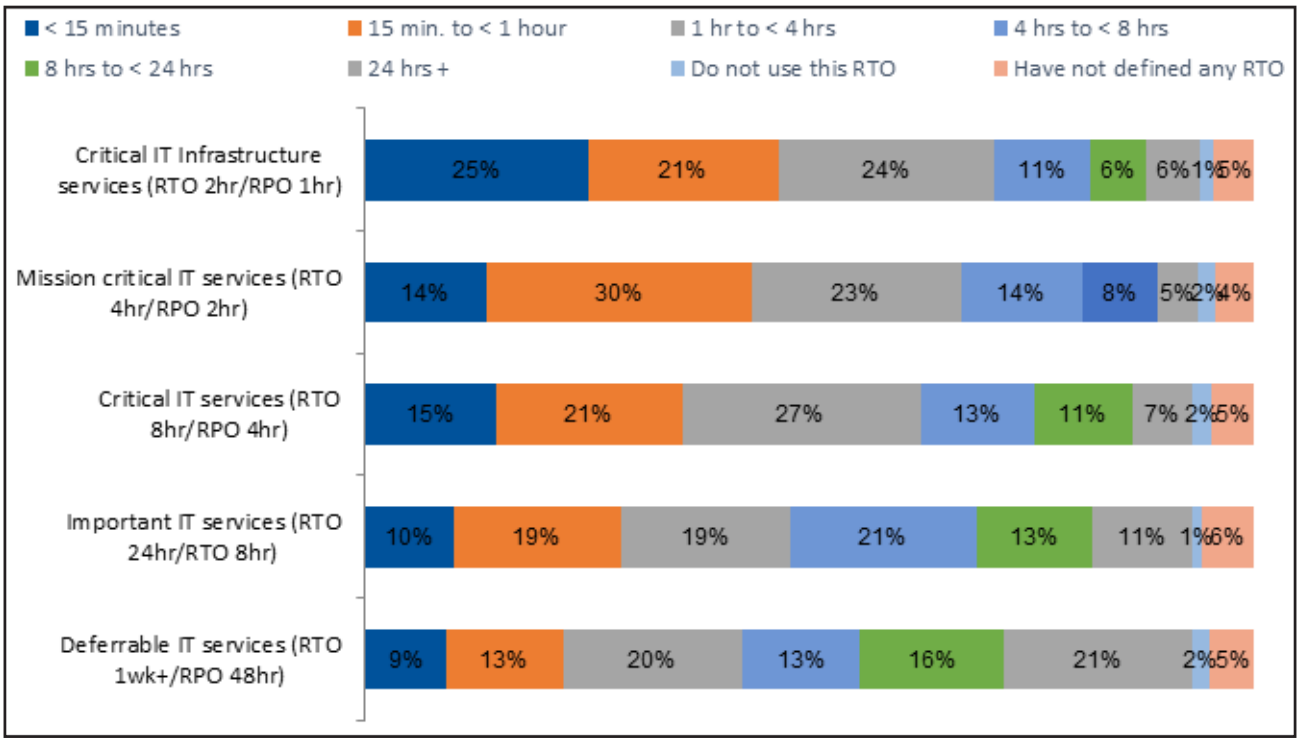
Next make sure you balance your desired RPO against your desired retention period. Also make sure your data protection solution can support technologies like SAN snapshots; you can achieve better data protection against logical failure when you have protection against physical failure, realized by moving sufficient data off your primary storage device.

Evaluate whether you have different RPO needs for different types of data. Typically structured data, such as databases and email, require a faster RPO than unstructured data. In addition, different clients might have need for different RPOs as well. Defining different RPOs for different types of data and systems is important.

Also, many people believe that RPO and RTO should be measured against all IT assets distributed throughout your company—not only those in the data center. Think about the RPO and RTO for the notebooks, workstations, and PCs in your environment. If you haven't included ALL of your IT assets, then you are leaving your company exposed in the event of a failure or disaster.

Lastly, be realistic about the RTO that you can endure. Every minute of an outage impacts your business and profitability. Provided as an illustration, based on a recent Gartner survey, additional information about RTO is show below. Note that the actual RTO timeframe sought was much less than originally stated.

What is the shortest time frame per recovery tier that your organization's applications or IT services fall into for the following Recovery Time Objectives (RTO)?



Data Protection is More Than Backup

Addressing Retention and Retrieval

Backup is critical. Let's assume that you sold the CFO on data protection and procured a purpose-built appliance, hosted in the data center. You feel you can meet your established RPO and RPO objectives under most circumstances. But the CFO asks: did you plan for data growth? What happens if you outgrow your solution in three months? And where are you going to put that data? You don't need short term access to it but what happens if you are audited? Do you have a backup of your backup? Better yet can you find the data you archived years ago? Every good data protection plan takes more than backup into account; you need to add data retention and retrieval elements to your data protection plan.

What Are the Regulatory Consequences of Data Loss?

Government regulations and associated compliance requirements impact data retention needs and retrieval plans. Regulatory compliance describes what corporations or public agencies must comply with in regard to relevant laws and regulations. CFOs care about regulatory compliance because the consequences of non-compliance range from corporate fines to the loss of personal freedom in egregious cases.

Regulatory compliance tends to vary by industry. For example, Sarbanes Oxley mandates that 7 years of financial data be retained while HIPAA states patient data must be available for the life of the patient and 2 years post-mortem. We identify some prominent regulations in Appendix B for your review.

Now you are convinced: provision more storage for data retention (we don't want regulatory compliance to come back and haunt us with associated financial penalties for non-compliance). Use possible penalty costs to justify a new, revised data protection solution with insurance or optimization. Yet what are the options for data retention?

The natural data path for the backup process is primary disk to secondary disk to tertiary disk or tape or other media off-site—or the cloud. This whole process is commonly described as 'disk to disk to X' (D2D2X) where X is disk, tape or other media; today X is increasingly cloud storage. No surprise that more IT departments are evaluating and selecting public cloud offerings for storage retention as private off-premise solutions grow more costly and variable.

Cloud storage is a great option for long term retention if you can find an affordable plan. The elimination of tape media can potentially offset this cost. Investigate cloud solutions that offer long term retention with optimal space allocation and a regular backup schedule. Vendors that offer primary backup and cloud storage give you the ability to migrate data between sites and create a more flexible backup schedule to stage your data and lower your cost more.

Remember that your choice of both media and site location will impact the total cost of your data protection plan.

Business Continuity and Disaster Recovery

Let's not forget business continuity. Do you have a disaster recovery plan in the event of a natural disaster or man-made outage—remembering that the probability of human error is greater? If yes, great. And while the disaster recovery plan looks good on paper, have you tested it to be sure the plan works as expected so you can achieve your established RPO and RTO goals?

Here are yet other alarming statistics:

Disaster Recovery Magazine's Preparedness Survey conducted in 2014 discovered:

- Worldwide, most companies put business operations at risk because they are not prepared to recover IT systems in the event of a disaster.
- Nearly three out of four organizations are at risk of failing to recover from a disaster or outage.
- Nearly two-thirds of respondents said their recovery plan and test did not prove useful under adverse conditions.
- Most organizations participating in the survey have not documented their disaster recovery plans or established key metrics such as RTO, RPO, failover and failback processes.

Continuity Central conducted a survey of business continuity professionals in the US, UK, Australia, New Zealand, Canada, and India in 2015. Their findings disclosed:

- Fourteen percent (14%) of respondents expect no changes in organizational business continuity (BC).
- Almost fifty three percent (53%) expect to see small changes in the next year.
- Thirty-three percent (33%) anticipate large changes in the way their organization manages business continuity.

Each respondent was asked to provide details of the one area likely to have the biggest impact on business continuity practices (BCP):

- Fourteen percent (14%) will be making major revisions to BC strategies and/or BCP(s);

- Nine percent (9%) will be introducing new business continuity software;
- Six percent (6%) will be implementing new IT DR, availability or cloud technologies;
- Six percent (6%) of respondents expect to see a significant increase in testing and/or exercising activities;
- Changes in the business / organizational structure will impact 6.1 percent of respondents;
- Five percent (5%) will embark on new ISO 22301 alignment, implementation and certification projects;
- Four percent (4%) will see their organization moving away from business continuity management to business resilience or operational resilience;
- Regulatory pressures and requirements are forcing changes in 4.1 percent of respondents' organizations;
- An increased focus on information security will be having an impact on 4.1 percent of respondents;
- There will be an increased focus on supply chain resilience / supply chain dependencies in 3.9 percent of respondents' organizations;
- Three percent (3%) will be rolling out business continuity awareness programs;
- Three percent (3%) of respondents' organizations will be taking a more formal approach to BCM;
- Two percent (2%) of respondents will be implementing a new automated notification system.

Top BCP challenges were lack of budget, funds, and resources as well as lack of top management commitment and buy-in/support. Recurring challenges were lack of business unit support, low priority in the budget and apathy.

Don't leave your company exposed. Exposure might cost you your job (remember Dynamic Markets' survey findings).

Now let's take a closer look at the test of a disaster recovery plan. A good plan should consist of the following items:

- Walkthrough Test – Team rehearses every step of the plan.
- Simulation Test – Pretend to test all hardware, software and personnel function including facilities.
- Parallel Test – In conjunction w/walkthrough or simulation, compare data, reports for accuracy.
- Full Interruption Test – Disable your system and see if the DR plan works. Expensive. Possibly disruptive.

Also necessary to recovery success are dedicated, empowered individuals, a stand-alone plan, and test post-mortems.

No surprise that the entire process of DR testing can be costly. Personnel, travel (between the primary site and off-site and then the regional and branch offices), plus actual downtime to test your plan add up to significant dollars. Is there a better option? Yes. Outsource your disaster recovery test. Let professionals maximize your plan and minimize your cost.

Look for a service that offers orchestration via replication as well as one that dynamically changes based on events and produces certified recovery points for the maximum control of your DR plan. The ability to restart quickly is key to meeting your RPO and RTO. A service that offers report verification gives proof that you selected the right solution.

Disaster Recovery in the Cloud

Finally let's take a closer look at Disaster Recovery as a Service (DRaaS).

As background, the DRaaS market emerged to address IT organizations' need to support increasingly aggressive recovery-time targets as well as more frequent, lower-cost testing. Early adopters were small

organizations with less than 100 employees lacking a recovery data center, experienced IT staff and specialized skill sets needed to manage a disaster recovery (DR) program on their own. DRaaS vendors provided VM recovery primarily for VMware but given the growth of other VM types such as Microsoft Hyper-V, Citrix Xen, Linux-centric KVM and Oracle VM (OVM), service instances grew heterogeneous. With increased customer demand for integrated support of hybrid recovery configurations (recovery configurations containing both virtual and physical servers) service offering have grown increasingly more complex, with increased subscriptions from a wide spectrum of small, medium, and large companies in all vertical industries.

Today there over 100 suppliers of DRaaS services offering failover to a cloud computing environment, either through a contract (SLA) or pay-per-use basis. The key to selection of a DRaaS provider is to ensure they meet your service requirements; don't assume a DRaaS provider will cover all disasters and deliver all possible services. The worst time to discover that the service provider cannot provide a required service is during a disaster.

We recommend that you look for a vendor that offers end-to-end protection, fast response, guaranteed SLAs, maximum security, and superior support. With benefits that include CAPEX (eliminate duplicate hardware and software requirements) and OPEX (fewer personnel to support alternate locations) savings, the time for a DRaaS has come.

Summary

There's no silver bullet to convince your CFO that data protection is vital to reduce the financial risk to your company. Use the insurance metaphor, a downtime cost calculation and need to comply with regulatory requirements will also be compelling. The best approach is extension of the insurance metaphor; illustrate increased productivity with optimization as it will build a bridge between you and your CFO as well as a shared understanding of risk and reward. Most important, it will show the CFO that you understand the financial side of data protection as well as secure a best "bang for the buck" solution.

APPENDIX A: Cost of Downtime Example

We will use the ESG (Enterprise Systems Group) approach to determine downtime cost as illustrated below:

Cost of Downtime = (*To* + *Td*) × (*Hr* + *Pr*) where

To = Time, length of outage
Td = Time, length of data loss
Hr = Labor cost $/hour
Pr = Opportunity $/hour

For our calculator, we will need 2 values each for the 2 variables noted (time, money) for a total of 4 data inputs.

First, let's derive the two types of time—lost data and outage time.

Lost Data Time

If a server fails, new data created since the last backup is potentially lost. Suppose our server failed at 2 p.m. on Wednesday and we assume a reliable restore from a successful backup on Tuesday night is available. We will presume that we lost data changed between 8 a.m. to 2 p.m. on Wednesday.

Td = Time of lost data (in this case is 6 hours)

We quantify lost data in a measurement of time because if it took 6 hours to create the data and assume it will take another 6 hours of business time to recreate it.

Outage Time

The server failed in the afternoon. We assume that end users are idle for the remainder of the day and the entirety of the next business day, Thursday. If this is true, the outage time is the remaining 3 hours of Wednesday afternoon plus all 9 business hours of Thursday. Note that we attempt to simplify all metrics in this example. Realistically, in today's economy—with international coverage and e-Commerce availability—the true downtime is more likely to be 27 hours (Tues 2p–Wed 5p).

To = Time of outage (3 + 9 hours = 12 hours)

Together, *To* + *Td* = 12 + 6 (or the total time attributed to server failure = 18 hours).

Now, we need to decide how much those 18 hours are worth, in dollars.

Next consider two types of costs—labor and opportunity cost.

Labor Cost

Assume that an end user is completely idle while the IT resources are offline. Also note that the company is essentially paying the salary or hourly wage of that person—for no benefit. We use simple hourly rates (unburdened without benefits added).

Hr = Hourly cost of impacted personnel ($ per hour).

In this example let's assume $40/hour. But perhaps the end user is not completely idle but impacted. Then take the hourly cost and multiply by .5 to show a half-impact (versus 100% idle and non-productive). Let's assume $20/hour for this example.

As every business is different, determine a $/hour number then apply this costs to the number of people impacted and unable to do their primary role due to an IT outage. Let's assume eight people are impacted in this example.

Hr = Hourly cost of impacted personnel ($ per hour) is $20/hour for eight people or $160/hour.

Opportunity Cost

Teams that create revenue cannot during an outage. The outage means lost opportunity. Determine the weekly or monthly opportunity of a team or monies that they generate/do not generate each hour and add that number to the equation.

Pr = Hourly opportunity cost (gain or loss $ per hour)

Our team produces $9,000 per day in revenue; their hourly 'cost' between 8 a.m. and 5 p.m. equates to $1,000 per hour.

Other examples of opportunity cost translated to revenue gains or losses—for this business—include:

- The service contracts team that needs to recoup losses if services are not rendered, and the SLA states fines are also imposed.
- The shipping department incurs penalties plus expedited shipping charges to make deliveries the day after the outage.

Again, every business is different. Assess a $/hour for the value that a team creates and then loses per hour noting some productivity is lost or penalties are incurred when the team is unable to perform their primary role due to an IT outage.

Calculate Down Time

Remember we determined our downtime equation to be:

Cost of Downtime = (*To* + *Td*) × (*Hr* + *Pr*) where

To = Time, length of outage
Td = Time, length of data loss
Hr = Labor cost $/hour
Pr = Opportunity $/hour

Applying the approximated values from our simple example in the downtime equation, we discover:

Cost of Downtime = (12 hours + 6 hours) × ($160/hour + $1,000/hour)
Cost of Downtime = (18 hours) × ($1,160/hour)
Cost of Downtime = $20,880

To = 12 hour outage
Td = 6 hours of lost data
Hr = $160/hour for the team to sit idle
Pr = $1,000/hour in lost revenue opportunity

APPENDIX B: List of Regulations for Compliance

Sarbanes-Oxley (SOX or Sarbox)

Sarbanes-Oxley established a set of regulations for all public companies in the United States. The applicable sections of SOX pertinent to data protection include:

Section 103: Auditing, Quality Control and Independence Standards - 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 provide resources to reduce identity theft. With respect to data protection, FACTA requires secure disposal of consumer information.

The 'Disposal Rule' specifically aims to protect the privacy of consumer information and reduce the risk of fraud and identity theft, and there is a federal rule that requires businesses to take appropriate measures to dispose of sensitive information derived from consumer reports—including backups.

GLBA (Gramm-Leach-Bliley Act)

GLBA is a comprehensive law that requires all U.S. institutions associated with financial transactions to protect the security, integrity, and confidentiality of consumer information. GLBA affects a 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 applicable to data protection are specified below (from the section of the law known as the "Safeguard Rule").

- Ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of such records;
- 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 an act that mandates security programs for all U.S. organizations that possess or use federal information systems on behalf of a federal agency. The act holds senior management accountable to ensure timely implementation of security measures. Viewing IT security as a life cycle process, FISMA integrates security with overall IT management and maintenance processes. The National Institute of Standards and Technology (NIST) outlines nine steps toward compliance with FISMA:

1. Categorize the information to be protected.
2. Select minimum baseline controls.
3. Refine controls using a risk assessment procedure.
4. Document the controls in the system security plan.
5. Implement security controls in appropriate information systems.
6. Assess the effectiveness of the security controls once they have been implemented.
7. Determine agency-level risk to the mission or business case.
8. Authorize the information system for processing.
9. Monitor the security controls on a continuous basis.

Government agencies are required to meet the standards published in the Minimum Security Requirements for Federal Information and Information Systems document (or FIPS 200) to heighten security within government information systems

HIPAA (Health Insurance Portability and Accountability Act)

HIPAA is a set of regulations applied to the U.S. health care industry. The major applicable requirements associated with HIPPA are as follows:

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

- Access to e-PHI 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.

HITECH (Health Information Technology for Economic and Clinical Health Act)

The goal of the HITECH Act is to promote the meaningful use of electronic healthcare records (EHR) in the healthcare system. Meaningful use is described below. There are monetary incentives for adoption and penalties for non-compliance specifically impacting doctors and hospitals who receive Medicare and Medicaid payments. HITECH was the impetus for the Health Information Exchange (HIE), a core capability for hospitals and physicians to achieve "meaningful use" and receive stimulus funding. Attributes of meaningful use include:

- Use of a certified EHR in a meaningful manner, such as e-prescribing.
- Use of certified EHR technology for electronic exchange of health information to improve quality of health care.
- Use of certified EHR technology to submit clinical quality and other measures.

In general, providers need to show they use certified EHR technology in ways that can be measured significantly in quality and in quantity. Specific examples of meaningful use are categorized as follows:

- Improve care coordination
- Reduce healthcare disparities
- Engage patients and their families
- Improve population and public health
- Ensure adequate privacy and security

There are a number of other regulations (and recommended certifications) that apply to non-U.S. entities including:

IT Infrastructure Library (ITIL)

ITIL, formerly known as the Information Technology Infrastructure Library, is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of businesses. ITIL describes processes, procedures, tasks, and checklists (not organization-specific) applied to integrate IT with an organization's strategy to deliver value and maintain a minimum level of competency. It allows the organization to establish a baseline from which to plan, implement, and measure. ITIL is used to demonstrate compliance and to measure improvement. Use of ITIL is resources is expensive and participation in certification programs is optional.

Data Protection Act 1998 (DPA)

DPA is an Act of Parliament in the U.K. that defines the law with respect to the processing of data on identifiable living people. The main piece of legislation to protect of personal data in the UK, it was enacted to bring UK law into line with the European Directive of 1995. It requires Member States to protect people's fundamental rights and freedoms, in particular their right to privacy with respect to the processing of personal data.

A summary of the key points of DPA follows:

- 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).

APPENDIX C: Cost Comparison Summary Sheet for CFO

Part 1

Cost of Downtime		Cost of Data Protection Solution
Cost of Downtime = (*To* + *Td*) × (*Hr* + *Pr*) where *To* = Time, length of outage *Td* = Time, length of data loss *Hr* = Labor cost $/hour *Pr* = Opportunity $/hour		Description of IT environment to protect Data center configuration Storage capacity Physical/virtual deployment Network capabilities Backup needs; established RTO, RPO Cloud capability and access for retention Disaster Recovery and Testing
Number of events/year Total Downtime Cost (Cost/Event X Number of Events)	vs.	Total IT data protection plan Cost of data protection solution

Part 2

Cost of DP Solution (from above)		Costs Saved due to Optimization of Resources
Description of IT environment to protect Data center configuration Storage capacity Physical/virtual deployment Network capabilities Backup needs; established RTO, RPO Cloud capability and access for retention Disaster Recovery and Testing		Onsite (due to appliance) Impact on CAPEX Reduction in footprint Reduction in storage needs Impact on OPEX Reduction in labor Reduction in facilities Off-site (due to cloud services) Impact on CAPEX, OPEX Off-site (due to outsourced DR services) Impact on CAPEX, OPEX
Total IT data protection plan Cost of data protection solution	vs.	Total Savings due to Optimization Total Savings due to Optimization