
Eren Unal
Bentley College,erenunal@gmail.com

David Yates,
Bentley College,dyates@bentley.edu

Follow this and additional works at: http://aisel.aisnet.org/ecis2010

Recommended Citation
ECIS 2010 Proceedings. 144.
http://aisel.aisnet.org/ecis2010/144

This material is brought to you by the European Conference on Information Systems (ECIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2010 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
ENTERPRISE FRAUD MANAGEMENT USING CLOUD COMPUTING: A COST-BENEFIT ANALYSIS FRAMEWORK

<table>
<thead>
<tr>
<th>Journal:</th>
<th>18th European Conference on Information Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manuscript ID:</td>
<td>ECIS2010-0452.R1</td>
</tr>
<tr>
<td>Submission Type:</td>
<td>Research Paper</td>
</tr>
<tr>
<td>Keyword:</td>
<td>Cost-benefit analysis, Software, Data security, Future of IS</td>
</tr>
</tbody>
</table>

*scholarONE™*  
Manuscript Central
Abstract

Enterprise fraud costs hundreds of millions of dollars every year. Enterprise fraud management (EFM) solutions analyze transaction data to see if it matches known fraudulent patterns. If it does, an alert is raised, and a fraud investigator is assigned to the alert. EFM solutions typically are sold as software products with a fixed-term license. We highlight best practices for these product-based solutions and consider an alternative architecture that leverages cloud computing. Cloud computing is an emerging system architecture where the user accesses software services using the Internet. Users only need Internet connectivity to utilize computation and storage services. Users needn’t know about the inner workings of the server software or the location of the servers. Thus, cloud computing relieves the user from the burdens of designing and building an in-house server architecture and purchasing licenses to run software. In this paper, we develop a framework that assesses the costs and benefits of enterprise fraud management solutions. We extend our framework to weigh the costs and benefits of EFM solutions deployed as a licensed product and also in the cloud. Finally, we present a cost-benefits analysis of comparable EFM solutions deployed using these two system architectures.

Keywords: Cloud Computing, Cost-Benefit Analysis, Enterprise Fraud, Enterprise Fraud Management, Value of Information.
1 INTRODUCTION

Whether it is check fraud, embezzlement or credit card fraud, enterprise fraud is a serious problem costing hundreds of million dollars every year. Financial institutions and high-net-worth individuals are subject to fraud generated by insiders, customers, and third parties. Enterprise fraud brings many issues with it: fraudulent activity itself costs financial institutions millions of dollars in lost revenue annually; fraudulent activity damages the reputation of banks and causes stocks to plummet; witnessing fraud leads honest employees to seek employment elsewhere, resulting in increased costs of attracting and retaining talent.

One way to do mitigate fraud is by using enterprise fraud management solutions (software) that analyzes the transactions taking place within the financial system. Transaction data that banks are comfortable with sharing are made available to the product multiple times a day. The product then analyzes the data to see if it matches any previously agreed upon patterns. Based on these patterns, if the solution detects fraudulent activity, then an alert is raised and an investigator is assigned to the alert.

Cloud computing is an up-and-coming architecture with strengths and room for improvement. Cloud vendors use a large number of identically configured, low-end servers to scale the computing supply. Cloud relieves the user from the burden of building a high-performing-server architecture, or purchasing licenses to run software, or building them in house. The cloud also offers “little compliance, recovery procedures, or transparency” (Heiser and Nicolett, 2008). There are no penalty clauses or SLAs that regulate the cloud. Financial institutions have strong financial incentives to pursue cloud investments, and are awaiting the cloud to improve its legal and operational accountability.

In the age of cloud, we believe that it is an outdated approach to consider software as a physical good or as a mere product. EFM solutions, except those by a handful of vendors e.g. Early Warning, are sold as a software product with fixed-term license. The product gets installed on the computers of financial institutions, behind their security defenses. When there is a problem with the software or the vendor wants to perform upgrades, the vendor has to access the installation behind the bank’s security defenses via secure means. However, the end goal for financial institutions is fraud mitigation and management services, rather than purchasing and maintaining fraud solutions as a product. The purchase, implementation, testing, maintenance, and recovery steps inherent to the traditional software-as-a-product model are all hindrances to catching fraud. Given that any two banks have similar enough transaction and reference data, all banks could pour their data into the fraud solution’s funnel under a cloud architecture deemed secure enough by all regulators and related parties.

In this paper, we have asked whether enterprise fraud management solutions are worthwhile. To answer this question, we have created a framework that weighs the costs of enterprise fraud to the cost-savings of enterprise fraud management solutions.

We have then asked, in the context of enterprise fraud management solutions, whether the cloud is a viable architecture alternative to the traditional software-as-a-product model. We have created another framework that measures the costs and cost-savings of enterprise fraud management solutions as a product and in the cloud. We base our frameworks on cost-benefit analysis and the value of information.

2 ENTERPRISE FRAUD

2.1 Enterprise Fraud: The Problem

Between April 1, 1996 and September 30, 2001, the Federal Bureau of Investigation received 154,062 Suspicious Activity Reports (SARs) for criminal activity related to check fraud, counterfeit negotiable
instruments, and related activity. These accounted for 27 percent of the 320,336 SARs filed by U.S. financial institutions, accounting for over $4.5 billion in losses (FBI, 2001).

In 2007, a teller at a U.S. bank was found to have created fraudulent transactions for six years using the general ledger. The employee stole over $3 million in that period (Santa Fe Group, 2007).

The U.K. Payments Administration Ltd. announced in March 2009 the annual card fraud figures for 2008. Card-Not-Present is a type of credit card transaction where the credit card is not physically present in the transaction. Card-Not-Present credit card fraud made up 54% of all credit card fraud cases in the U.K. in 2008, accounting for £328.4m in fraud losses.

A senior executive of a global bank was caught in 2007 for embezzling from client accounts. The theft was discovered three years after it began, and the bank was fined more than $700,000 by local regulators for inadequate fraud detection and prevention controls (Santa Fe Group, 2007).

In 2007, the stock price of a subsidiary of a top 100 U.S. financial institution went down by 50% following the announcement of a collusion of its senior executives to commit loan fraud. The parent company had no real means of monitoring the activity of its subsidiary by subverting internal controls. As a result, the institution faced costly lawsuits and hard losses of over $140 million. The institution was ultimately acquired at a significant discount (Santa Fe Group, 2007).

Whether it is check fraud, embezzlement, or credit card fraud, enterprise fraud is a serious problem costing hundreds of millions of dollars every year. Enterprise fraud brings many issues with it: fraudulent activity itself costs financial institutions millions of dollars in lost revenue annually. Fraud that becomes public knowledge damages the reputation of banks and causes stocks to plummet (Santa Fe Group, 2007). Furthermore, witnessing fraud leads honest employees to seek employment elsewhere, which results in increased costs of attracting and retaining talent (Santa Fe Group, 2007).

2.2 Enterprise Fraud Management Software: A Solution

It is in the best interest of financial institutions to take measures to mitigate fraudulent activity, even if they couldn’t fully eliminate it. One way to do mitigate enterprise fraud is to use detection and prevention software that analyzes the transactions taking place within the financial system. The input that any bank account fraud detection and prevention system needs is transaction data. Transaction data that banks are comfortable with sharing are made available to the product daily on a regular interval. The product then analyzes the data to see if it matches any previously agreed upon patterns. If a fraud pattern is detected, then an alert is created and an investigator is assigned to the alert.

3 CLOUD COMPUTING

Cloud computing refers to an architecture where the user accesses software using the Internet. To receive these services, users only need sufficient infrastructure to connect to the vendor’s servers. Users needn’t know about the inner workings of the software or the location of the servers. Staten et al. (2008) suggest that most cloud providers fall into one of the two categories: Internet services companies and hosting providers.

3.1 Benefits of the Cloud Architecture

Cloud computing offers high economies of scale and skill (Schadler, 2008). The leading cloud vendors buy server, storage, and other equipment in bulk. As such, they have a much higher negotiating power when it comes to hardware pricing, software licensing, and support contracts (Staten, 2008). Cloud vendors use a large number of identically configured, low-end servers to scale the computing supply. Cloud vendors keep these servers at the most economically feasible location(s). Cloud relieves the user from the burdens of building a high-performing-server architecture, purchasing licenses to run software, and building software in house. Processing, storage and retrieval are offloaded to the vendor who specializes in performing these tasks in an efficient manner.
The cloud could also be viewed through the dilemma of whether to outsource. According to Dodd and Martorelli (2003), one must list the “activities and values that form the essence of the organization’s brand(s) and value propositions(s)...” These will determine “what needs to be an integral internal function and what can be wholly or partially sourced elsewhere”. If data storage and processing are not among the core “activities and values” of a company, then the company is better off outsourcing these services to a vendor who will deliver it better, safer, cheaper or faster.

In the software-as-a-product model, customers have to post the hardware and software assets on their balance sheets and depreciate them. Cloud shifts the value proposition of software from code to delivery of capabilities through a service. The service of software is purchased on a need basis. In a world where the cost of maintaining software is four times the cost of purchasing and implementing it (Carr, 2008), a hosted, on-demand model to access software effectively reduces the user’s capital expenditure in physical infrastructure and software.

Most cloud vendors charge by the use of resources in processing hours, gigabits consumed, and gigabits per second transferred, rather than by a monthly fee. Staten cites (2008) that, according to Michael Crandell, CEO of RightScale, whereas the average monthly cost of a server is $400 for an enterprise, it is only $70 to $150 for Amazon, a benchmark vendor of scaled and efficient computing power.

Prentice argues that cloud computing shifts some of the control over the terms and pricing of software from vendors to users (2008). Software, when purchased as a product, comes with an end user license agreement, which is an obligation on the user. Software purchased or used as a service, however, comes with service level agreements (SLA), which are obligations on the vendor. The more offerings there are on the cloud, the more downward pressure there will be on industry margins. Also, with long-term software license commitments out of the picture, customers at any time could choose not to extend their cloud service subscriptions.

3.2 Room For Improvement In The Cloud

The cloud offers cost-savings through economies of scale. Vendors gain flexibility by avoiding specifics about its location, staff, processes, technology, and subcontractors. Heiser and Nicolett argue, however, that the same characteristics that make cloud offerings scalable also make it hard to assess the degree to which providers can and will provide confidentiality, integrity, and availability (2008).

Although it is always possible for trusted employees to go bad and commit fraud, and it is not automatically the case that outsiders are less ethical than employees, it is prudent to put more trust in co-workers than those who do not have a long term commitment in the enterprise. When data is hosted outside the enterprise or handled by non-employees, internal controls over who accesses data and how it is accessed are bypassed. It is harder to obtain information from a vendor than a co-worker. Also, according to Heiser and Nicolett (2008), while vendors might hire a trusted profile of employees, if data is not encrypted and it can be read at the vendor’s site, it should be assumed that it will be read.

Heiser and Nicolette agree that the cloud offers “little compliance, recovery procedures, or transparency” (2008). There are no penalty clauses or SLAs that regulate the cloud. Most privacy laws and regulations assume that, in any given case, the entire set of data is hosted in a single country. Countries have different regulations, dispute resolution practices, and crime rates. In the event of data theft, data can flow from the jurisdiction of one country to the next almost too easily before authorities of the two countries can cooperate. Financial institutions have strong financial incentives to pursue cloud investments, and are awaiting the cloud to improve its legal and operational accountability.

3.3 EFM In The Cloud

When it comes to EFM, the end goal of financial institutions is fraud mitigation itself. Purchasing fraud solutions as a product and maintaining them are means to an end. However, the purchase, implementation, testing, maintenance, and recovery steps inherent to the traditional software-as-a-product model are hindrances to catching fraud.
It is a daunting task for any EFM vendor to implement their solution under the EFM-as-a-product model, i.e., behind a bank’s security defenses. Although any two banks could be argued to store similar information about their customers, transaction and reference data that any two banks store will be different from each other in terms of the number of data fields provided and the types of data fields, length of data fields, and other attributes. Therefore, each bank gets a custom installation of essentially the same product, and each bank has to allocate a portion of its valuable computation cycles to fraud detection, multiple times a day. Although EFM solutions are designed to process large volumes of data (tens of gigabytes daily), they occasionally “break” and cause, if nothing else, a downtime on the schedule of fraud investigators waiting for new alerts to look into. This downtime not only costs the bank, but it is usually caused by the bank itself, as well. If the bank’s computer systems are tied up with more important tasks that day and the EFM solution loses priority, the solution does not have enough computation cycles to process the raw data. As a result, the product “breaks”, and fails to populate the inbox of fraud investigators and analysts with new alerts. Furthermore, the return on investment on the product is reduced for reasons that could have been avoided by the bank.

The malfunction of the EFM-as-a-product solution is similar to the broken copier situation: The copier is the “product” that the company bought from a vendor. The product is on company premises, so when the product breaks, the company has to call the vendor and wait for the mechanics to arrive. The company might be able to fix a copier themselves; but the company is not likely to be qualified, encouraged, or allowed to fix an EFM solution without the vendor’s help.

Based on the potential need for EFM solutions and the cloud as an architecture alternative, the question of whether EFM could be done in the cloud naturally springs to mind. Although each bank might have different internal systems, workflows, data types, and data retention policies, there is a finite set of financial services provided and financial principles and enough aspects must be similar between any two banks if they operate and are regulated in the same environment. Therefore, banks could pour their data into the fraud solution’s funnel under a cloud architecture deemed secure enough by all regulators and related parties. In the age of cloud, it is an outdated approach to consider software as a physical good or as a mere product.

Under the EFM-in-the-cloud model, large volumes of raw transaction and reference data could be sent to the cloud EFM vendor multiple times a day over secure connections. Under service level agreements (SLAs) between the bank and an EFM vendor, the vendor would have to protect the confidentiality and integrity of the information, and deliver alerts to fraud investigators and analysts in a timely manner.

Cloud can drastically improve the return-on-investment of an EFM tool. The financial institution that we will be using in our paper has market capitalization of, roughly, $700mn in the NYSE. We were told that this bank utilizes EFM solutions that catch 50 to 75% of all fraud. Under the EFM-in-the-cloud model, this rate is expected to reach a drastically higher 75 to 90% of all cross-institution fraud, if the vendor has access to data from all banks involved. It happens that 50 to 55% of all fraud is cross-institutional, where the fraud is committed using the lag time that funds take to transfer between institutions.

Carr argues (2008) that computing and storage are seen as commoditized services, much like factories that once created their own power but now tap utility grids. Carr also analyzes the improvements in illumination: it all started with the torch, which led to the invention of the candle. Then there was the gaslight, followed by the incandescent light bulb. We have had the highly efficient, light-emitting diode for decades now, which is slowly being replaced by the organic light-emitting diode. Unlike light, or a physical product, however, electricity does not need to be created or stored where it will be used. It can be outsourced and used as often as needed.

Computing has become a utility that does not need to be created in house. Information systems have seen many improvements, from punch card inputs to keyboards and monitors, to voice input and output. If the final goal of such systems is to process, store and access information, it makes perfect
sense for these services to be provided by someone who can do it in the cheapest and most scalable way.

In The End of Software, Chou finds standardization through repeatability and automation key to improving processes (2004). Fraud prevention consists of a repeatable and automated set of processes, and would therefore lead itself to on-demand or cloud solutions.

3.4 Concerns Performing EFM Using Cloud Computing

The primary concern before implementing EFM-in-the-cloud would be security; financial institutions are renowned for their reluctance to share data and give up control over operations, which is what the cloud involves (Scott, 2009). Most cloud vendors’ terms of service spell "If something goes wrong, you can’t blame us" (Urquhart, 2009). A hacker or a third-party user with administrative rights could attempt to access, modify, destroy, render inaccessible, or destroy data for financial gain (Coblentz, 2009). A natural disaster, power outage or other unexpected situation could render datacenters unavailable (Coblentz, 2009). When data, datacenters, or services are unavailable, banks could lose revenue during the down time, which might cause customers to take their business elsewhere (Coblentz, 2009).

Financial institutions are not going to jump to cloud solutions overnight just to reduce data processing and storage costs. For financial institutions to invest in cloud solutions, the cloud should mature and become more accountable. Data could be encrypted prior to being transferred to, and stored at datacenters, and stored at multiple datacenters, ideally in multiple countries (none of which are hostile to the customer’s country) (Coblentz, 2009). Cloud consumer protection laws could be passed, and cloud malpractice lawsuits could be allowed (Urquhart, 2009). Banks could employ security experts and engage in independent assessments on the security of networks and datacenters (Coblentz, 2009).

4 RESEARCH QUESTIONS AND METHODOLOGY

4.1 Research Questions

Regarding cloud computing architecture and the need for enterprise fraud management (EFM) solutions, we ask the following two questions:
1. Are enterprise fraud management solutions worthwhile?
2. Is it appropriate to operate enterprise fraud management solutions in the cloud?

4.2 Methodology

Our goals were to first quantifiably assess the value of investing in an EFM solution to a bank, and then determine whether it makes sense to deploy such a solution in the cloud. In an effort to achieve these goals, we perform a cost-benefit analysis, carefully considering the value of information.

4.3 Value Of Information

The value of information is critical to our work since enterprise fraud management (EFM) is about financial institutions trying to protect sensitive information, and EFM solutions require financial institutions to share this information with an EFM solution provider in a secure manner. When a company shares information with another company, or undertakes the responsibility to securely process, store and access sensitive information, the company is charged with investing in technical and human resources to protect the 1) confidentiality 2) availability and 3) integrity of the information (Gordon and Loeb, 2006). Furthermore, two additional concerns tied to the identity of users who access information are authentication (making sure that a user is who they claim to be) and non-repudiation (making sure that a user cannot, at a later time, deny that they have accessed the information).

Gordon et al (2006) argue that information sharing networks are designed for the main purpose of increasing the number of users accessing information conveniently. They are not necessarily designed to secure information. Sensitive information is subject to threats and vulnerabilities (Gordon et al,
Threats are actions or events that might lead to information security breaches: For example, current or former employees might decide to sell strategic information or customer identities; outsiders can hack into a company’s systems and steal information. Vulnerabilities are weaknesses of a system that increase the likelihood of success of an attack on the system: For example, storing sensitive information without encryption and access control encourages attempts to steal such information and increases their likelihood of success.

In determining how to allocate resources to protect information, direct vs. indirect costs and explicit vs. implicit costs need to be understood: Direct costs are those that can be tied to individual breaches, and include personnel, software, and hardware related costs that can be associated with a breach. Explicit costs are those that can be monetarily quantifiable in an unambiguous way. These include technology-related costs (e.g., incurred in deploying firewalls, encryption, access control, intrusion detection, etc.) and human resource costs (e.g., incurred in the design and implementation of technological solutions, etc.). Implicit costs, however, are costs associated with lost opportunities. One example of an implicit cost is legal liability that might result from a security breach. Another implicit cost would be the damage to the reputation of the company as a result of a breach. Implicit costs are more difficult to quantify.

4.4 Cost-Benefit Analysis: Net Present Value

In a project where the benefits are harder to name and to quantify than the costs, the terms benefit, cost-displacement, and cost-avoidance often have the same meaning (Campbell and Brown, 2003). Gordon et al (2006) view the benefits of a cybersecurity investment as the costs that do not occur, or the cost-savings realized through the investment. Throughout our paper, we use the terms benefit and cost-savings interchangeably.

It is important that we differentiate between operating expenses and capital expenditures in our analysis. Operating expenses benefit a single period’s operations, usually one fiscal year. Capital expenditures represent assets, appear on a company’s balance sheets, and usually benefit a company for a term longer than one fiscal year. The portion of a capital expenditure that is lost during a fiscal year is charged to that period as an operating expense. Both types of expense are captured as costs in the following formula which determines the Net Present Value (NPV) of a project (Sassone and Schaffer, 1978):

\[
NPV = \frac{B_0 - C_0}{(1 + d)^0} + \frac{B_1 - C_1}{(1 + d)^1} + \ldots + \frac{B_t - C_t}{(1 + d)^t} + \frac{B_n - C_n}{(1 + d)^n}
\]

*Equation 1 Net Present Value Formula*

where

- \(B_t\) is the dollar value of benefits incurred at time \(t\),
- \(C_t\) is the dollar value of costs incurred at time \(t\),
- \(d\) the discount rate, and
- \(n\) the life of the project, in years.

To determine the economic attractiveness of a multi-year project, all streams of benefits and costs incurred in different periods need to be reduced to a single value today, using a discount rate that a company uses to evaluate other capital investment decisions (Campbell et al, 2003).

The interpretation of the NPV of a project is as follows:
1. Engage in the project if its benefits outweigh its costs;
2. Do not to engage in project if its costs outweigh its benefits; and
3. In the event that the benefits of a project are equal to its costs, be indifferent towards the project.
4.5 Net Present Value of EFM Investment

To take into account the initial up-front investment and the sum of the net benefits beyond the initial investment, Gordon et al (2006) adapt Equation 1 to the context of cybersecurity investments as follows:

\[ \text{NPV} = -C_0 + \sum_{t=1}^{n} \frac{(B_t - C_t)}{(1 + d)^t} \]

Equation 2  Net Present Value of a Cybersecurity Solution

where

- \( C_0 \) is the cost of up-front investment in the cybersecurity solution,
- \( C_t \) the dollar value of costs incurred at time \( t \),
- \( B_t \) the dollar value of benefits incurred at time \( t \),
- \( d \) the discount rate, and
- \( n \) the lifetime of the solution, in years.

We use Equation 2, Gordon and Loeb’s (2006) methodology of cost vs. cost-savings of a cybersecurity investment, in calculating the cost and cost-savings of performing EFM. EFM solutions require secure components – secure applications, secure databases, secure servers, secure networks etc. – to be effective. Furthermore, the core mission of EFM solutions – to prevent and detect fraudulent transactions – is closely related to cybersecurity, which, in general, is about preventing and detecting security breaches. As for cybersecurity, EFM “benefits” are about cost-savings.

4.6 Our Framework

To answer our first research question, we have enumerated the costs and cost-savings of investing in an EFM solution:

<table>
<thead>
<tr>
<th>Costs of EFM solution</th>
<th>Cost-savings from EFM solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up-Front Investment</td>
<td>Hard Losses Recovered (FBI, 2001)</td>
</tr>
<tr>
<td>Annual Operating &amp; Maintenance Costs</td>
<td>Litigation Liabilities Recovered (Gordon et al, 2006)</td>
</tr>
<tr>
<td>Hard Losses Sustained (FBI, 2001)</td>
<td>Business Loss Due To Discouraged Customers Recovered (Santa Fe Group, 2007)</td>
</tr>
<tr>
<td>Litigation Liabilities Sustained (Gordon et al, 2006)</td>
<td>Employee Turnover, Talent Attraction and Retention Costs Recovered (Santa Fe Group, 2007)</td>
</tr>
<tr>
<td>Business Loss Due To Discouraged Customers Sustained (Santa Fe Group, 2007)</td>
<td>Less, Lost Employee Productivity (Santa Fe Group, 2007)</td>
</tr>
<tr>
<td>Employee Turnover, Talent Attraction and Retention Costs Sustained (Santa Fe Group, 2007)</td>
<td></td>
</tr>
</tbody>
</table>

Table 1  Framework for Costs of and Cost-Savings from EFM Solutions

In an effort to answer our second research question, we have taken the costs and cost-savings from Table 1 and incorporated them in a comparison of deploying EFM as a product and EFM in the cloud:

<table>
<thead>
<tr>
<th>EFM-as-a-product</th>
<th>Costs</th>
<th>Cost-savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up-Front Investment</td>
<td>Annual Operating &amp; Maintenance Costs</td>
<td>Hard Losses Recovered (FBI, 2001)</td>
</tr>
<tr>
<td>Litigation Liabilities Sustained (Gordon et al, 2006)</td>
<td>Employee Turnover Costs Recovered (Santa Fe Group, 2007)</td>
<td></td>
</tr>
<tr>
<td>Business Loss Sustained (Santa Fe Group, 2007)</td>
<td>Employee Turnover Costs Recovered (Santa Fe Group, 2007)</td>
<td></td>
</tr>
<tr>
<td>Employee Turnover Costs Sustained (Santa Fe Group, 2007)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EFM-in-the-cloud</td>
<td>Annual Service Fee (Carr, 2008)</td>
<td>Hard Losses Recovered (FBI, 2001)</td>
</tr>
<tr>
<td>Bandwidth Lease (Carr, 2008)</td>
<td>Litigation Liabilities Recovered (Gordon et al, 2006)</td>
<td></td>
</tr>
</tbody>
</table>

In an effort to answer our second research question, we have taken the costs and cost-savings from Table 1 and incorporated them in a comparison of deploying EFM as a product and EFM in the cloud:
Service Level Agreement
Hard Losses Sustained (FBI, 2001)
Litigation Liabilities Sustained (Gordon et al, 2006)
Business Loss Sustained (Santa Fe Group, 2007)
Employee Turnover Costs Sustained (Santa Fe Group, 2007)

Business Loss Recovered (Santa Fe Group, 2007)
Employee Turnover Costs Recovered (Santa Fe Group, 2007)

Table 2 Framework for Costs of and Cost-Savings for EFM-as-a-product and EFM-in-the-cloud Solutions

4.7 Limitations Of Our Framework
A cost-benefit analysis of EFM solutions is only one view into whether or not deploying such a solution would make sense for an enterprise. In the broader context of business risk management, such analysis might be considered hand-in-hand with other analyses such as expected rate-of-return, payback-period or cutoff period (Sassone and Schaffer, 1978) which are beyond the scope of this paper. Generating a complete list of costs and benefits is difficult, especially since for information technology projects this process is vulnerable to errors of omission (Remenyi, 1999). Accurately quantifying costs and benefits is also challenging. The first problem here is that IT projects can transform business processes and transformation of business processes requires costs that are hard to measure and delivers benefits that also are hard to measure. The second problem is avoiding double-counting (especially of benefits). Finally, some IT-driven cost savings are difficult to measure, e.g., measurements that depend on answering questions such as “how much time is saved by automating a process via method A versus B?” when neither method is currently implemented. Furthermore, we assume that the EFM projects in this paper are both feasible (e.g., are not constrained by capital costs) and are independent of other projects (Sassone et al, 1978).

5 RESULTS

5.1 Our Assumptions
When weighing costs against cost-savings, we assume the following:
• The term of the project (also the end-user license of the EFM solution under the EFM as a product model) is 3 years.
• The bank we choose to use in this scenario has market capitalization of $700mn in the NYSE, $80bn in assets, 120,000 employees, 2,500 branches and 30,000 ATMs in the United States and more than 40 offices around the world.
• The bank uses a discount rate of 10% to evaluate projects.
• The bank takes hard losses of $1 million dollars each year for the next three years (Santa Fe Group, 2007). The EFM as a product solution can detect 50 to 75% of the fraudulent activity whereas the EFM in the cloud solution can detect 75 to 90% of all cross-institutional fraudulent activity (that is, 50 to 55% of all fraudulent activity).
• At the end of the third year, the bank is fined with legal liabilities by regulators. This figure is $700,000 (Santa Fe Group, 2007) when there is no EFM solution, $700,000 * % of undetected fraud under the EFM as a product model, and 1.5 * $700,000 * % of undetected fraud under the EFM in the cloud model.
• When the news breaks at the end of the third year, the bank loses an additional $2mn as customers decide to take their business elsewhere (Santa Fe Group, 2007).
• The bank’s stock crashes due to bad publicity and loses 50% of its market capitalization at the end of the third year (Santa Fe Group, 2007).
• 10 employees of the bank, each earning $100,000 a year, resign at the end of the third year because they lose faith in their employer. The true cost of employee turnover is twice the annual salary of the employee (Santa Fe Group, 2007).
• An up-front investment of $261,129 under the EFM as a product model that includes the following:
  o EFM solution license fee of $200,000 (for a three-year license);
Five Windows 2003 Server R2 Enterprise Editions at $3,999 (Microsoft, 2009a) for a server with 25 client access licenses (for fraud investigators and analysts); and

- SharePoint Server license at $41,134 (Microsoft, 2009b).

- Under the EFM in the cloud model, an annual service fee paid to the EFM solution vendor of 104,452, or 40% of the up-front investment under the EFM as a product model.

- Under the EFM in the cloud model, to negotiate a Service Level Agreement (SLA) that includes reasonable guarantees about secure transmission, processing and storage of transaction data and also customer data, the bank pays legal fees of $75,000.

- Under the EFM-in-the-cloud model, the bank uses a T3 connection to send data to and receive alerts from three data centers of the EFM solution vendor, at $6,000 dollars per connection per month (Dedicated Circuit Pricing, 2009).

- Under the EFM as a product model, operating costs for the bank to operate 6 servers are $400 per server per month (Staten et al., 2008).

- There is a loss of productivity when the EFM as a product solution fails due to lack of computation cycles. We have assumed this to be 5 analyst hours per week for an analyst that earns $120,000 a year and works 40 hours a week.

We have determined each dollar value above from the source shown in parentheses or from our own experience. We believe these values are reasonable and, in fact, realistic values for our study.

### 5.2 Costs Of EFM Solutions vs. Cost-Savings From EFM Solutions

Using the assumptions above, we compared the costs of deploying an EFM solution against the cost savings from using an EFM solution (see Table 1), discounting cash flow where necessary. Our cost-benefit calculation shows that the cost-savings from investing in a three-year EFM solution exceed its costs by almost $3mn (see Table 3).

<table>
<thead>
<tr>
<th>Cost of EFM solution</th>
<th>Cost-Savings from EFM solution</th>
<th>NPV</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5,192,818</td>
<td>$8,099,395</td>
<td>$2,906,577</td>
</tr>
</tbody>
</table>

Table 3 Cost of, Cost-Savings from, and NPV of EFM Solutions

The benefits (i.e., cost-savings) from investing in an EFM solution exceed the cost of the investment by $2,906,577. Based on this analysis, we conclude that it makes sense for a bank operating in an environment similar to the one captured by our assumptions to invest in an EFM solution, from a cost-benefit standpoint. We therefore answer our first research question as follows: **It is worthwhile to invest in enterprise fraud management solutions.**

### 5.3 NPV Analysis Of EFM As A Product and EFM In The Cloud Solutions

Notice in Table 2 in the costs of EFM-in-the-cloud solutions that some of the familiar capital expenditure cost items of EFM-as-a-product solutions are replaced by operating expenses inherent to the cloud. The cost-savings items listed in EFM-in-the-cloud solutions are almost identical to the cost-savings items of EFM-as-a-product solutions. “Cloud” and “product” are computed identically, using Equation 2. However, the resulting dollar value that is calculated using Equation 2 in each case is different, due to the different operational efficiencies each architecture yields.

<table>
<thead>
<tr>
<th>Costs</th>
<th>Cost-Savings</th>
<th>NPV</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFM-as-a-product</td>
<td>$5,192,818</td>
<td>$8,099,395</td>
</tr>
<tr>
<td>EFM-in-the-cloud</td>
<td>$4,296,164</td>
<td>$9,460,931</td>
</tr>
</tbody>
</table>

Table 4 Costs of EFM-as-a-product and EFM-in-the-cloud Solutions

By applying Equation 2 and making the assumptions in Section 5.1, we determined that the cost savings of investing in an EFM in the cloud solution exceed its cost by $5,164,767. Based on our analysis, we conclude that it makes sense for a bank operating in the business environment described above to invest in an EFM in the cloud solution. Furthermore, the analysis presented in Table 4 shows that the cost of an EFM in the cloud solution is less than that of an EFM as a product solution, and that
the cost savings from an EFM in the cloud solution exceeds the cost savings from an EFM as a product solution. Thus, our NPV calculations show that cloud computing is the most beneficial and least costly of the two architectural alternatives for operating an EFM solution. Thus, our second research question is answered in the affirmative, specifically: We recommend that EFM solutions be deployed in the cloud based on their cost-benefit performance.

6 CONCLUSIONS AND FUTURE WORK

We have described the gravity and magnitude of enterprise fraud as a problem, and considered enterprise fraud management software solutions to this problem. We developed a cost-benefit analysis framework, considering the value of information, for enterprise fraud management. We have applied our framework to analyze the costs and benefits (i.e., cost-savings) of investing in an enterprise fraud management solution. We have demonstrated, under real-world assumptions, that it is worthwhile to invest in enterprise fraud management solutions. We have also shown that cloud computing is a useful architectural alternative to product-based implementations and expanded our framework to compare the performance of enterprise fraud management as a product to the performance of enterprise fraud management in the cloud. By a margin of more than 40%, our findings indicate that cloud computing is a more beneficial and less costly architecture with which to implement enterprise fraud management when compared to custom-installed, software as a product architectures.

We expect that in the broader context of business risk management, our cost-benefit framework, when accompanied by expected rate of return and payback period analysis, will make a compelling case for EFM solutions in general and also EFM solutions in the cloud in particular. This is the main focus of our future work. Other possible directions for future research include better aligning EFM solutions with market requirements, addressing technological and operational concerns, and performing more advanced cost-benefit analysis (e.g., sensitivity analysis).

EFM solutions are only as good as the fraud they catch, and metrics for this purpose need be developed beyond those presented in this paper. Ideally, an EFM solution should maximize the number of true positive alerts, and minimize the number of false positive and negative alerts. Furthermore, when, how, and in what form alerts are reported to the company and the EFM solution vendor are important operational concerns that need to be addressed.

We will also be tracking and assessing the maturity of different cloud architectures, platforms and implementations that can host and process data of the sensitivity and volume present in the financial services market. For cloud computing to serve financial institutions, its solution providers must process, store, and retrieve such data with the necessary business continuity, regulatory compliance, recovery procedures, and transparency. We expect that as cloud computing meets these challenges the business case for EFM solutions in the cloud will evolve and become even more compelling.

ACKNOWLEDGEMENTS

The authors would like to acknowledge Tim Brady, Paddy Kalathur and Paul Reed, who all made insightful and important contributions to this paper.
References


