July/September 2011 BLUEKAIZEN.ORG Issue 3 Vol 1

SecurityKaizen

your way to improve your security

EXCLUSIVE INTERVIEW WITH JOE SULLIVAN FACEBOOK.COM CSO

EXCLUSIVE INTERVIEW WITH AL BERMAN DRII.ORG CEO

BUSINESS CONTINUITY IN THE MIDDLE EAST

SECURITY KAIZEN TEAM IN HITB AMSTERDAM

Are you prepared for a DISASTER?

SecurityKaizen magazine

Media Sponsor

for

2011

Information Security Conferences

Conference	Date
Hacker Halted, Cairo	December 2010
TakeDowncon, Dallas	May 2011
HITB, Amsterdam	May 2011
MENA ISC, Jordan	September 2011
Cairo Security Camp	October 2011
HITB, Kualalumpur	October 2011
RSA, London	October 2011
Hacker Halted, Miami	October 2011

Register Now on www.bluekaizen.org and have the oppurtunity to **win free tickets** to our sponsored Conferences

Chairman & Editor-in-Chief
Moataz Salah

Editors
Mahmoud Tawfik
Moataz Salah
Omar Sherin
Vinoth Sivasubramanian
Mohamed Mohieldeen
Mohammed Farrag

Web Site Design
Mariam Samy

Arabic Translator
Mai Alaa El-Dien Saud

Graphic Design
Mohamed Fadly

Security kaizen is issued every 3 months

BLUE KAIZEN

For Advertisement in Security Kaizen magazine and www.bluekaizen.org website:
Mail: Info@bluekiazen.org
Phone: 010 267 5570

Editor's Note

It has been 6 months since our first issue. Looking back, I can see how the magazine has evolved throughout these months, and how the community is growing. The first issue was downloaded 900 times in 7 days and the second issue was downloaded 2700 times in only 3 days. I know I was surprised at how many of the people at the CairoICT event knew about our magazine; it was great to talk in person to so many of our readers.

We were able to media-sponsor some renowned conferences, such as TakeDownCon Dallas and HITB Amsterdam. Sponsoring helps us to step up our presence not just in Egypt and the Middle East but to take Security Kaizen magazine outside the MENA region and get more readers from the USA and Europe. Also, that gave us the opportunity to interview the chief security officer of Facebook, Joe Sullivan.

Representatives from Mozilla, Google, Microsoft, and Adobe are now aware of Security Kaizen Magazine. We started to catch the eye of the security community in the whole world. And I have all my readers and dedicated team to thank for that.

In our 3rd issue we will try to make it more special by focusing on one topic. The recent events in Egypt and the Middle East have been quite dramatic and unusual, presenting unprecedented challenges to business operations and especially IT systems. One major lesson-learned from this situation is the need to have resilient plans for Business Continuity and Disaster Recovery, so this theme is the focus for the new issue.

And to make the 3rd issue more special, I am happily announcing that this is to be the first printed issue of the magazine, so as promised and as we are always trying to kaizen we were able to improve in every issue. The first issue was released in January 2011 and despite the conditions in Egypt during this period, we were able to release the second issue in April with two versions, an English one and an Arabic one, and finally our special third issue is to be printed allowing you, our devoted readers, to read it at your convenience.

Moataz Salah
Bluekaizen Co-founder

Security Kaizen

July\ September 2011 . 3rd Issue

True Story

new&News

Interviews

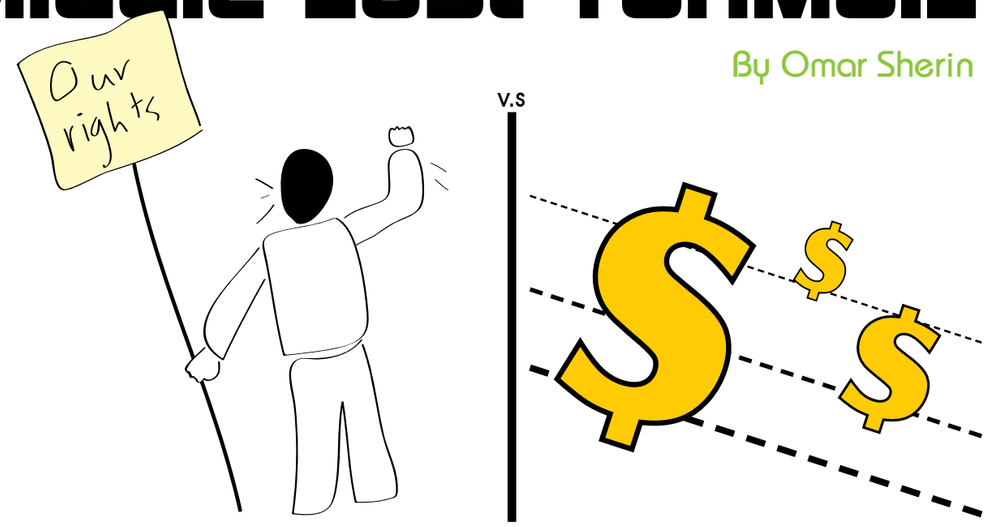
Best Practice

Photos of cover by: Mohamed Fadly

BUSINESS CONTINUITY

Amidst the Recent Middle East TURMOIL

By Omar Sherin



In the past few weeks, the Middle East has been the scene of unprecedented and rapid political and social changes that took even the most mature businesses and industries by surprise, and left them virtually paralyzed.

Not even the most sophisticated and knowledgeable secret intelligence agencies predicted the massive scale social uprisings that are emerging throughout the region.

It is worth analyzing business continuity strategy in Egypt because the country witnessed probably the first international incident ever recorded for a government actually using the internet "kill switch"[1] as well as the ripple effect of consequences resulting from the decision. Additionally, as Egypt is the second strongest economy in the African continent (following South Africa), it has the most diversified economy in the region by United Nations standards; therefore, the impact on diversified businesses is clearly visible and is not sector-specific.

How Business was Impacted

After days of continuous anti-government demonstrations that used the Internet and social networks such as Facebook and Twitter as coordination platforms, the former administration decided to cut the Internet minutes before midnight on January 27th with the hope of preventing protesters from using their communication tools.

Minutes later, it was confirmed that there was no Internet connectivity whatsoever across the entire country. What was once deemed technically impossible was proven to be technically possible. In such authoritarian countries, much of the physical telecommunications infrastructure is under the direct ownership and control of the government.

We saw firsthand the catastrophic impact of the government's impulsive decision. Imagine a country or a modern business deprived "overnight" of emails, VoIP services, e-commerce, online conferencing, browsing the web, running a corporate website or even seeking or providing remote online support. This unprecedented situation lasted for 5 consecutive business days.

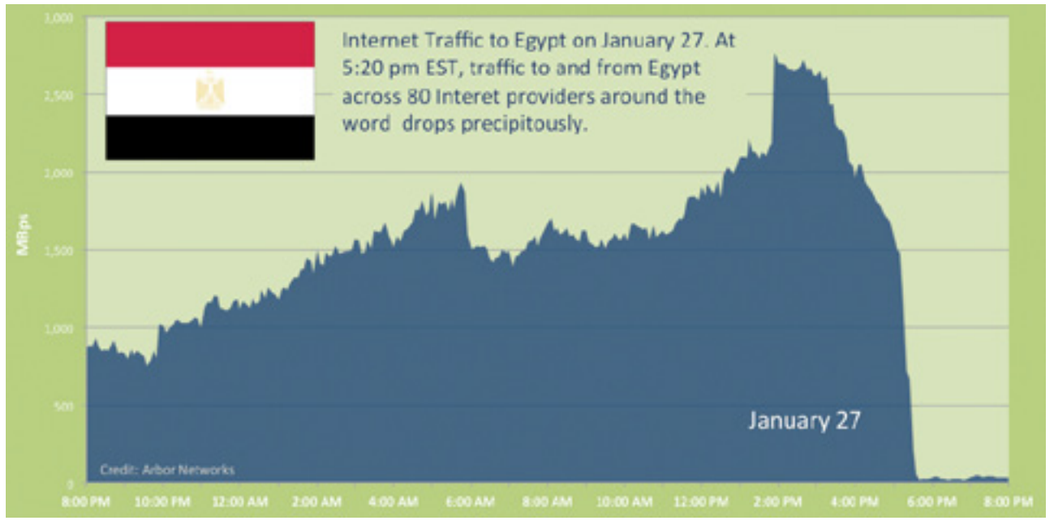


Figure 1 - Internet Cut Off on January 27th

Immediate Impact

Companies working in the IT outsourcing industry were amongst the first to be affected. Recently released official OECD statistics 4 estimated that the direct loss in revenue in those five days ranged from $90 million USD to $120 million USD which does not include lost business opportunities and possible SLA violations and lawsuits.

Another example is the banking sector. Several national and multinational banks announced key services such as international money transfer and online banking were unavailable or unreliable. With the national ATM network shutdown and the standalone ATM machines vandalized, millions of bank customers resorted to standing in long queues in front of their local bank branches. Unfortunately up until now there aren't any formal studies on the implications of the shortage of cash flow on small businesses.

How Business Continuity Plans Were Exercised

Very few companies appeared to be resilient and unaffected. Some companies survived due to exercising solid Business Continuity Plans (BCPs) yet others were sustained just because of pure luck.

One particular and major mobile operator is a good example of a company that survived the disruptions due to a solid and comprehensive Business Continuity Plan.

On January 27th, the BCP was triggered by the government cutting off the Internet. Then the Crisis Management Team (CMT) got together and activated the Disaster Recovery Plan (DRP) to safely shut down the local IT services and focus on securing the physical assets, data centers, key cellular towers, power generation stations, from sabotage and perhaps looting due to riots and clashes in the streets.
Initially, the customer call center was bombarded with complaints about difficulties using communication services like mobile Internet, Blackberries and even international calls. Although the customer service representatives tried to explain the situation to callers, they later realized it was a national problem.

On January 28th, the government announced a national state of emergency and a curfew was enforced. Furthermore, all the mobile operators in the country received orders from the government to shut down all mobile communications including voice and SMS services as a last attempt to cripple the demonstrators' communications.

Due to a provision in the mobile regulatory license agreements signed with all the mobile operators, companies had to comply. This decision proved to have significantly costly and negative corporate image implications because the general public perceived this action from the telecommunication operators as a gesture of aiding the previous authoritarian regime and taking sides against their own customers. In the last few weeks there has been several customer and civil rights activists grouping people and

calling for a national day boycotting the mobile service for 30 minutes as well as filing tens of law suits against the operators,

At this stage the Crisis Management Team ordered the shutdown of the customer call center and landlines, activated the internal call tree and ordered all staff to remain at home until further notice.
After receiving confirmation that all headquarters and branch offices countrywide had been evacuated and locked, the CMT started the Crisis Communication Plan (CCP). A key requirement of the CCP was to deliver relevant status update messages to international media and foreign stock markets where the company is listed.

On the IT side of the disruption, the DRP of this company was designed to mitigate the risk of total and complete loss in connectivity by developing a replica of its web services hosted in Europe as well as by signing with a prominent cloud-based managed services provider to manage the security and availability of the corporate emails for its 5,000 users. This managed service had a provision that allowed them to save drafts of undelivered emails "in the cloud" for up to seven days. Once the former president and his administration announced his resignation, the Internet was back online and the employees' mailboxes were flooded with week-old emails, a situation certainly better than getting an empty mailbox and a handful of angry customers.

On the other hand, entities such as the Egyptian Stock Exchange (egyptSE.com) and some banks which appeared to be online and reachable throughout the Internet blackout proved to be on a single and fairly small ISP in terms of market share (about 8%) called Noor Group5. Noor Group was clearly the exception. It is unclear whether the ISP survived the former government's decision by coincidence or perhaps due to its strategic list of customers including the likes of the Stock Exchange.

Based on available information, nearly 80% of the businesses in Egypt did not list the scenario of a national Internet blackout as a strong possibility and accordingly were unprepared.

The remaining 20% of companies were either well prepared with alternative and varied means of international communication such as satellite connectivity "VSAT" or companies that do not exclusively rely on the Internet for business.

Who Survived?

As most advanced secret intelligence agencies in the world such as the CIA did not anticipate this revolution "as far as we know", the United States Secretary of State Hillary Clinton described[1] the Egyptian government as "stable" even after three days of dramatic events. Interestingly, none of the traditional risk assessment methods available or practiced in most of the companies in Egypt would have predicted such a risk of major political overhauling and social uprising.

Interestingly this is a world premiere of a government using the Internet "kill switch" coupled with nationwide mobile communication blackout. And that simply caught everyone off guard.

Corporate risk experts should have learned from their previous experience in 2008, when there was a major Internet services disruption caused by an undersea Internet cable cut[3].

Failing to anticipate and include this major incident in the corporate risk matrix is impermissible.

Perhaps the only companies which continued operation throughout the January 2011 events "until announcing the state of emergency and general curfew" were the ones with rigorous, dynamic and active risk assessment practices that learned from the 2008 events and used or translated those lessons into viable disaster scenarios. Apparently it's not as easy

as it sounds as most companies faced problems, especially when it comes to developing a feedback system to ensure that the organization continues to review, incorporate and learn from experience dealing with new and emerging threats that were unthinkable or unprecedented two years ago.

One key observation is that companies that used Cloud Computing were noticeably more resilient and capable to work around this disruption because of the flexibility and availability offered by the Cloud Computing architecture.

Cloud-Based Availability

The cloud-based high availability architecture allows companies to outsource the management and maintenance of their critical systems like email for example and move the email archiving and high availability functions to the Cloud. As in the diagram below (Figure 2)

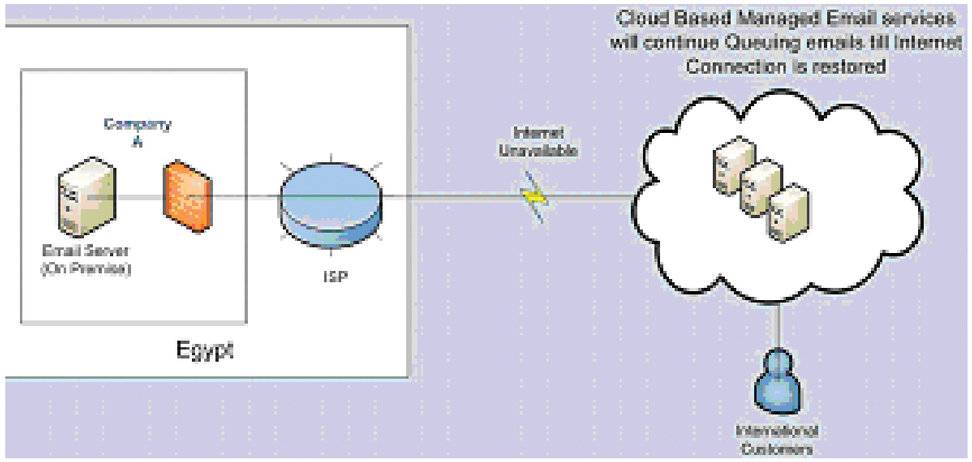


Figure 2 - Cloud based managed email system

The system safely and securely archives external emails in the cloud. Thus in case the corporate in-house email server becomes unavailable as in the case of internet blackout, the cloud-based managed email service would act on the company's behalf and continue to receive and queue emails addressed to the company (while actually offline), all this is transparent to the sender, for example international customers. This ensures that your corporate image remains intact with no business opportunities lost.

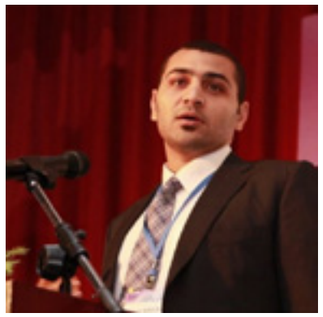
Traditional BC/DR Practices Shortcomings

Many small to mid-sized businesses with traditional BC and DR plans found that their plans had many shortcomings

dealing with this particular situation as there was a dependency on modern technology. Ironically, many companies could not activate their call trees as mobiles and SMS were unavailable, and disseminating a message to the branch offices across the country was nearly impossible.

Even companies with expensive disaster recovery sites (located over 100 miles away) had problems activating the DRP due to the complete and prolonged loss in connectivity and the inability to seek technical support from partners or vendors, including industry blue chip companies.

The recent events emphasized how modern businesses really depend on technology and particularly the Internet along with the unfortunate reminder that we take these modern technologies for granted.



About the author:

Omar Sherin

I am a certified CBCP, CRISC and ISO27001LA and in my spare time an active blogger in (ciip.wordpress.com).

References:

1 Internet Kill Switch (http://www.infowars.com/egypts-internet-kill-switch-coming-to-america/)
2 Hillary Clinton comment on the events on the 28th (http://af.reuters.com/article/topNews/idAFJOE70O0KF20110125)
3 Undersea cable cut (http://news.bbc.co.uk/2/hi/7792688.stm)
4 OECD statistics on cost of internet shut down (http://www.pcmag.com/article2/0,2817,2379324,00.asp)
5 Why is Noor Online? (http://www.huffingtonpost.com/2011/01/31/egypt-internet-noor-group_n_816214.html)

Figures:

1 Internet Kill Switch – Source: Arbor Networks
2 Cloud based managed email

A Visit to HITB

By Moataz Salah

HITBSECCONF2011

For those who don't know about Hack in the Box (HITB), here is an introduction. HITB is a well-known IT security organization that conducts three major conferences each year, in Malaysia, the Netherlands, and this year, India instead of the UAE.

As part of our ongoing mission to bring the latest in information security events to the attention of our readers, Security Kaizen served as a media sponsor for the HITB Amsterdam event. Our team attended the two day conference and took advantage of the opportunity to interview experts and transfer the picture as much as we can for those who couldn't attend.

It was a good experience to be at an international conference where security professionals from all over the world are gathered with the sole purpose of sharing their knowledge and expertise.

From the organizing perspective, Amsterdam is a great choice as a venue for the conference. Amsterdam is one of the most popular destinations in Europe, as it is one of those places that offer a variety of attractions and activities to do in your free time.

The choice of the hotel was spot-on. It is located in the heart of Amsterdam on the very famous Dam Square, so it was hard to get lost trying to find the hotel, and being in the center of Dam Square allowed attendees to easily

take short tours around the city after the sessions.

The conference started with a speech from Joe Sullivan, the Chief Security Officer of Facebook.com. He focused on the security threats that Facebook handles every day, and described how Facebook's employees have recently launched a number of unique security features that leverage the social graph. He also mentioned the blocking of Facebook access during the recent events in Tunisia, Egypt and Syria. I won't get into the details here, as you can have a look at the exclusive interview that Joe did with Security Kaizen Magazine in this issue.

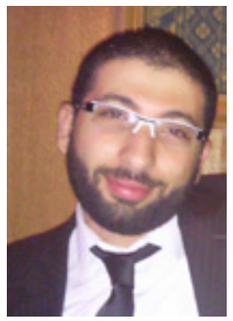
After this session, the conference was divided into 3 different tracks, each covering a different topic, and you had to choose one from the three. To be honest, I didn't like that idea because I wanted to attend different sessions that conflicted with their timings. Also the number of attendees was not that big, so after dividing them into three rooms, some sessions might have only 10-15 people, which didn't look so good.

A good example of a presentation was "Malicious PDF Analysis"; the session was presented by Didier Steven (Security Consultant Europe NV). It was a 2 hour lab session full of practical activities to explain how to analyze a malicious PDF using a step-by-step process starting from Exercise 1on how to extract a hidden message in a PDF file up to Exercise 12 which showed how to extract the malicious code. The instructor provided all the attendees with a DVD containing a VM machine, tools, documents and exercises, even more than the ones done in the lab, to be tested at home. I have to admit that this session was the most beneficial for me at HITB Amsterdam.

The second day started with a panel discussion on "The Economics of Vulnerabilities" featuring representatives from Google, Microsoft, Mozilla, Adobe and Blackberry. It was a very lively discussion between the audience and the speakers, as some of the audience could not understand why vendors are not rewarding freelance researchers who discover the vulnerabilities in their products, especially given the alternative and more lucrative black market for vulnerabilities. In the absence of a positive rewards system, it is difficult to blame vulnerability researchers for turning to the black market and getting substantially more for their efforts than even the competition programs such as Google's provide. The discussion was fun and it showed clearly the fact that the black market for vulnerabilities really exists, and the most important thing is that it is really profitable.

At the end, HITB Amsterdam was a good experience, and you could feel the warmth, the love and the effort of all the HITB crew. Also I have to thank Dhilon (founder of HITB) for all his effort, and the great crew he built. What a lot of people don't know is that the HITB crew members are all volunteers, motivated by sharing information and knowledge-spreading concepts.

Wish you all luck in attending the next HITB in Malaysia!



About the author:

Moataz Salah

I am the founder of Security Kaizen Magazine; Building knowledge is my target

BlueKaizen

Mail: info@bluekaizen.org

To get HITB material: http://conference.hitb.org/hitbsecconf2011ams/materials/

ArabBSD

The New Evolution for Arab Operating System Developers

By Mohammed Farrag

ArabBSD is a project which aims to increase the awareness of operating system development and help Arab operating system developers in BSD environment starting from the analysis of FreeBSD operating system infrastructure, formulating block diagram and calling for research groups in each track.

The need for working in stable track has become a desire for many programmers. The comprehension of the Operating System programming pays programmers attention and leads them to highly classify it.

Also, OS programming requires intelligence for applying constraints from software on hardware and providing compatibility between different peripherals and processor and this make a competition for those who like challenges. Simply, Operating System acts as intermediate layer between software and hardware. Any change to the Kernel APIs will affect higher layer application to be either not running or running incorrectly. In Operating System, you can select the best suitable environment for your code, i.e. cloud, filesystems, embedded, security, DataBase and or network programming.

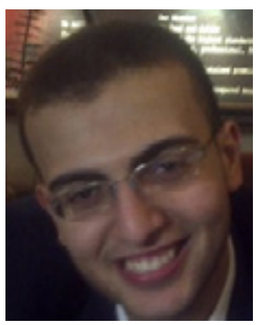
The work in ArabBSD is accomplished in two parallel directions. The first is the translation of FreeBSD documentation and its learning tutorials into Arabic beside the website translation. The second is offering free summer training for starting work on FreeBSD development. But Why BSD Systems?!

Berkeley Software Distribution (BSD, sometimes called Berkeley Unix) is the UNIX derivative distributed by the University of California, Berkeley, starting in the 1970s. The name is also used collectively for the modern

descendants of these distributions.

BSD was widely identified with the versions of UNIX available for workstation-class systems. This can be attributed to the ease with which it could be licensed and the familiarity it found among the founders of many technology companies during the 1980s. This familiarity often came from using similar systems—notably DEC's Ultrix and Sun's SunOS—during their education. While BSD itself was largely superseded by the System V Release 4 and OSF/1 systems in the 1990s (both of which incorporated BSD code), in recent years modified open source versions of the codebase (mostly derived from 4.4BSD-Lite) have seen increasing use and development. FreeBSD is classified as one of the most reliable and secured operating systems according to http://news.netcraft.com. Also, the availability of FreeBSD core team members and their full cooperation lead us to consider it as the development environment. I didn't forget to mention that CISCO and Yahoo servers are "FreeBSD Machines".

Regarding the current progress, some work in tutorial translation field has achieved and we are working hard for better. Finally, anyone who is interested in operating systems and their news can join us on our website https://sites.google.com/site/arabbsd/ , our facebook group or our Google mailing list. Members will keep up with operating systems issues for both administration and development including mastering all types of programming.



About the author:

Mohammed Farrag

ArabBSD Project Manager, FreeBSD Contributor, Google Technology User Group Administrator, GTUG Magazine Project Manager.

Recent Hacking Incidents in Egypt & Middle East

In this article, we have collected a few of the cyber attacks that happened in Egypt or Middle East on Governments, Banks and Media in the last few months. We would like to thank Osama Kamal for his efforts in helping us collect all this data.

The content of this article does not reflect Security Kaizen's opinion on the matters. We are simply stating some of the reported incidents.

This page was h@cked

Media Sector

Sunday, 5th of June 2011, Akhbar el yom website was hacked

The Akhbar Al Youm newspaper website was hacked because of a cartoon by Mustafa Hussein and Ahmed Ragab about a Salafi trend in Egypt. The hacker claims that he is not a Salafi but a Muslim and he does not accept mocking other Muslims and ladies wearing Neqab. He even said that no one dares to mock the Christians in this way wondering how the newspaper calls for dialogue, tolerance and freedom of expression while they mock Muslims. He is angry and is wondering why the women wearing Neqab were mocked despite it is their personal freedom.

Friday, 4th of February 2011, AlJazeera.net Website was Hacked

AlJazeera and other news agencies have been working so hard during the last few months to cover the Egyptian and Tunisian revolutions. However, some people didn't like the way that AlJazeera handled this coverage to the limit that it was blocked from the NileSat. That's why an anonymous hacker hacked Aljazeera.net website and wrote the following message "Together to bring Egypt down".

Wednesday, 30th of March 2011, ON TV Website was hacked

The ON TV website has been hacked by an anonymous hacker called A-Alexand. The message left at the website says:"The marriage of power and money produces corruption, no for money exploitation to control power and politics... Yes for Egypt free from corruption". He also sent out a warning to Naguib Sawiris, the owner of the channel, to stop launching a campaign against Islam.

Government Sector

June 2011, Login Passwords for Government Websites in Bahrain, Egypt, Jordan, and Morocco Were Published Online

A list of Egyptian government agency e-mails including Ministry of Communication and Information Technology, NTRA, IDSC and others have been breached. This incident was reported by Security Kaizen to EGCERT and they proceeded with their investigations. The same was done in Bahrain, Jordan and Morocco.

June 2011, Bahrain Governments' Websites Attacked

Hackers have launched a series of attacks on government websites after the country was granted the right to stage the Gulf Air Bahrain Grand Prix.
The Northern Governorate website, the official government tourism website and others have been hacked. Pictures of wounded anti-government protesters were visible if users clicked on categories on the main page of either website.

April 2011, Website of Municipal Council of Elections in Saudi Arabia was Hacked

The attacker was successfully able to change the main home page of the website and add a message to King Abdallah ben Abdelaziz asking for help from the injustice of the traffic system in the attacker's city, stating that he suffered a lot from it and is nearly bankrupt!

Financial Sector:

May 2011, HSBC Egypt Bank Phishing Attack

A Phishing mail was sent from customer_service@hsbc.eg with the subject: Update Your Account. The message requested that the user click on the link attached in the mail to receive an urgent message, otherwise the user's online banking would be blocked.

April 2011, Abu Dhabi Islamic bank

A Phishing mail was sent from customerservice@adib.ae with the subject: SECURITY NOTICE asking the user to follow a certain link to use the new upgraded SSL database of the bank instead of the old one.

Dubai First Bank

A Phishing mail was sent from service@dubaifirst.com with subject: Your Online Banking Has Been Blocked with a link attached to reactivate your account. As with all Phishing attacks, the attached links guide you to the attacker's website not the real bank website.

References:

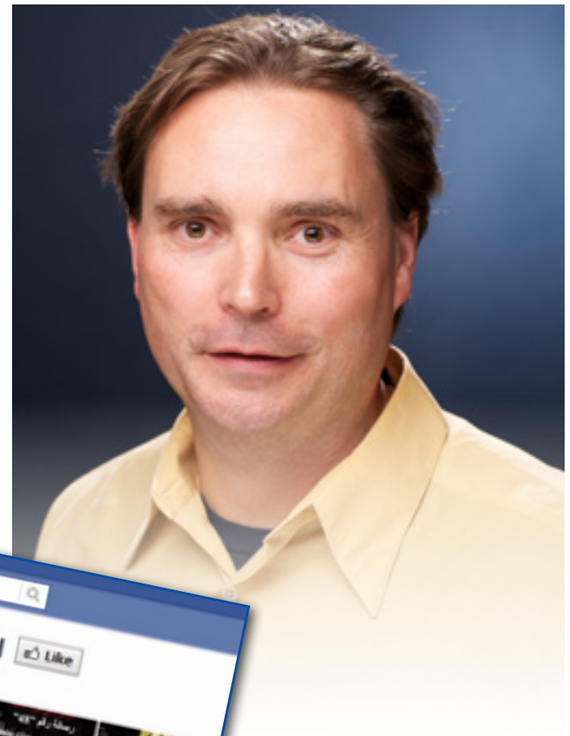
http://egyptianchronicles.blogspot.com/2011/06/akhbar-al-youm-website-is-hacked.html
http://egyptianchronicles.blogspot.com/2011/03/ontv-website-is-hacked.html
http://www.aljazeera.net/NR/exeres/07E58207-E080-414F-9C52-5C7D57CB6205.html
http://www.tradearabia.com/news/IT_200063.html
http://pastebin.com/n98jDJMq
http://www.tech-beat.com/719/
http://www.fraudwatchinternational.com/phishing/individual_alert.php?fa_no=239311&mode=alert
http://www.fraudwatchinternational.com/phishing/individual_alert.php?fa_no=239214&mode=alert
http://www.fraudwatchinternational.com/phishing/individual_alert.php?fa_no=239048&mode=alert

This page was h@cked

Interviews

Interview with
Joe Sullivan,
CSO of Facebook.com

By Moataz Salah



Today, Facebook is one of the most popular websites in the whole world, especially in the Middle East. It is one of the best-known examples of the new phenomenon of "social networks", where users voluntarily share information and their personal histories, with stories and regular updates on their daily lives, along with photos of family and friends, their connections, and more. With so much personal information shared in social networks, and so many data breaches in the news, the privacy of Facebook has become a real concern. Facebook.com is also credited with playing a main role in the Arabic Revolutions in the last few months. The increased use and impact of Facebook amongst the general population has prompted entities such as the Egyptian Army and other government agencies to create official pages on Facebook.

That's why it was mandatory for the Security Kaizen team to conduct this interview with the Chief Security Officer of Facebook.com, Mr. Joe Sullivan, and try to learn more details about Facebook security. Moataz Salah, Security Kaizen Editor, met with Joe and asked him the following questions.

Can you please introduce yourself to Security Kaizen readers?

I'm Joe Sullivan, the Chief Security Officer at Facebook. I manage a few of the teams at Facebook focused on making sure that people who use Facebook have a safe and positive experience.

Prior to joining Facebook in 2008, I spent 6 years working in a number of different security and legal roles at PayPal and eBay. Before that I worked for the US Department of Justice for 8 years. I was very lucky to have the chance to be the first federal prosecutor in a US Attorney's office dedicated full-time to fighting high-tech crime. I was privileged to work on many high-profile Internet cases, ranging from the digital evidence aspects of the 9/11 investigation to child predator, computer intrusion, and economic espionage cases. I was also a founding member of the Computer Hacking and Intellectual Property Unit, a special unit based in Silicon Valley dedicated exclusively to high-tech crime prosecution.

Can you give us an overview of the Security Teams in Facebook, the role of every team and the average number of employees per team?

We have over 30 people on the Security Team, but that really understates the number of people working on Security at the company. Facebook has engineering, risk, compliance and operations teams outside of Security that are also 100% dedicated to security and safety. Together there are hundreds of us focused on the area. Within the Security Team, we divide up into functional groups such as product security, investigations, information security practices, and law enforcement relations.

What kind of daily activities do you handle?

Facebook Security has a wide range of duties ranging from keeping our physical environment and electronic data safe to helping maintain the integrity of the site. We work internally to develop and promote high product security standards, partner externally to promote safe internet practices, and coordinate internal investigations with outside law enforcement agencies to help bring consequences to those responsible for spam, fraud and other abuse.

What is the most challenging incident you have faced recently?

Our biggest challenges come when we have to disprove negatives. There are so many security "experts" writing about Facebook we are constantly responding to claimed vulnerabilities that turn out to be theoretical at best. Just in the last month there were two stories that received global media coverage where if you had read the headlines you would assume that major security breaches had happened. In fact, in neither case had a security vulnerability lead to harm to a single person.
We also deal with really unique challenges that require speed and creativity. The situation in Tunisia (when ISPs started inserting code into our login page) stands out in my mind, because it was something we had not seen before but were able to roll out a complete incident response plan (including launching coding changes on our site) in under five days.

Do different governments including the US government ask for your help in certain Cyber Crime cases? Examples?

Someone on my team talks to a government official from somewhere in the world almost every day of the week—and that should be no surprise. These interactions range from the typical sharing of cyber crime trends, to participation on investigations, to dialogue about content standards, to responding to requests for user records. We try to foster positive dialogue so that we understand government concerns while always maintaining our commitment to respecting the privacy and security rights of our users.

What was your action plan during the recent situations in the Middle East when some countries blocked Facebook?

Our primary focus throughout this time was on maintaining account security and integrity. We cannot counter a decision to shut down internet access altogether or block access to our site but we can focus on preventing unauthorized access to accounts.

To avoid future similar incidents, what kind of updates did you have to your contingency plan?

We continue to focus on measures to give people more control over the security of their account. We launched opt-in HTTPS and hope to make HTTPS by default soon. We now offer Login Notification, Login Approvals (a form of two-factor authentication), Social Verification, One-Time Passwords and Remote Session Control to give all our users the tools to safeguard their accounts. To complement these user-facing tools, we constantly iterate on our technical systems which consist of multiple proprietary programs that classify malicious actions, roadblock compromised accounts, scan URLs and maintain the integrity of the site.

Why you should attend Cairo Security Camp 2011?

Excellent Speakers

Cairo Security Camp 2011 will bring you some of the best Security Expert speakers in Egypt and MENA area. Presentations and panel discussions on the most recent security topics will be held for two days.

Did you notice attacks to specific protesters' profiles or specific groups during this period either from the old Egyptian government or the Tunisian government?

One silver lining on all of this has been that the same tools we rolled out years ago to prevent Phishing and other types of account takeovers work equally well in combating other types of attempts to compromise accounts. But out of respect for the privacy of each user, we have not publicly discussed specific cases.

Do you think governments have the right to cut the Internet connections and what do you think the response of US citizens would be in such a case?

Through our growth as a service used by hundreds of millions of people in every country in the world, we have shown the power of the Internet as an indispensable tool for communication. To the extent we believe communication and access to information are fundamental to a just society, we should always be concerned when access is denied.

Interview with

Al Berman,

CEO of DRII.org

By Moataz Salah & Omar Sherin

Can you introduce yourself to Security Kaizen readers?

I have been the Executive Director for DRI International for the last five years. Prior to that, I was the Business Continuity Management Global Head for Marsh and prior to that I was the Operational Resilience Director for PwC. Additionally, I am the former CIO of a major bank, as well as a former CEO.

Can you please introduce DRI International as an organization and the role the DRI members play in the various industries/professions?

DRI International is a non-profit organization, which for the last 23 years has been dedicated to preparedness around the world. We are the largest certifier and educator of people in Business Continuity. We serve on committees all around the world. We teach in 45 countries, in eight languages, and we have some 8,500 certified professionals in more than 100 countries and in every industry and profession.

Does DRI International play a role in supporting conferences covering Business Continuity and Disaster Recovery (BC/DR)?

DRI has been involved in conferences all around the world. In fact, I recently returned from a conference in Brazil, of which one day (DRIDAY) was dedicated to DRI certified professionals discussing their roles in their organizations. And at the end of June, I am attending a conference in Brussels. DRI has spoken at conferences in Spain, Mexico, Singapore, the United States, and Malaysia in 2011 alone. And in 2012, DRI International will be having its own conference in May in New Orleans.

Can you give us an update as well as your insight onto the recent activities centered around BC regulations and standards worldwide?

We've seen a number of new standards and regulations around the world in business continuity, and most of them turn out to be a reaction to an event. 9/11 was a big impetus in the United Stated, but we're seeing it all over the world. Every central bank has a business continuity requirement. There are British standards (BS 25999), U.S. standards (NFPA 1600), and there are other standards as well. The new evolving standard, ISO 22301 will be another attempt at creating an ISO standard to replace BS25999.

But we are starting to see more regulations, and they come out of major events. If you look at the events in the United States recently, the Dodd-Frank Bill – which is to deal with the economic crisis – has business continuity in it. FINRA, which is the financial regulatory body in the United Stated, just passed regulation 4370, which also covers business continuity.
But what we're seeing is the real understanding that businesses have to be prepared for emergencies, and they have to go through the planning process so they can maintain the viability of not only their business but also everybody else's. And recent incidents in March in Japan, for example, showed how incidents affect supply chains around the world.

Do you think the new and emerging BC/DR standards will also focus more about the recovery of the technology environment as most standards haven't been historically?

I think there are a lot of standards about technology; ISO 27001 is totally focused on technology. But I think, to some extent, you're right. The new ISO standard 22301 will replace BS 25999. As you probably know, BS 25999 does not contain IT recovery. So, I think there is significant understanding that technology is an instrumental part of recovering all operations.

In your opinion what will the new ISO 22301 try to improve and stress compared to the current BS-25999?

I think the obvious one is technology recovery, which is missing from BS 25999. I also think that it is more broad-based, being an international standard, as opposed to being a strictly British one. It provides a broader framework in which to work. I think it's certainly an improvement over BS 25999.

But as most people know, standards themselves are not as strong as regulations. And I think we're going to see more regulations. When you look at regulations, they are prescriptive so they tell you what to do. And they are performance-based, so they you how to measure what you are doing. Standards, on their own, do not do that. They only serve as a basis of comparison, from best practices to how you are doing at your organization.

After the recent conditions in the Middle East and also the huge earthquake disaster in Japan, do you think that organizations that use the Cloud concept will be a step ahead?

I think what the Cloud concept does is distance you from a particular incident. What we saw, in Japan in particular, was the ability for financial system to continue to operate even in those areas that were devastated by the tsunamis. So, I think the answer to that is yes.

However, in the Middle East, one of the big problems when we looked at the recent disruptions in Egypt was closing down the Internet. Closing down the Internet would not have helped you continue to work even if you had Cloud technology. So, as long as communications are available, Cloud technology certainly is a better way of doing things, especially in a crisis.

In the wake of the recent ME events, how would you prioritize the biggest concerns for organizations that are in the region now?

Obviously, we have great concerns about people, but I think technology is a very big component of what is needed. We need to make sure technology is available so that you can communicate within the country and without the country. I think we need to understand that there have to be plans in place and there have to be resources that you can utilize outside of the affected area. So, I think what we're really saying is that we do need a great deal of planning, and more importantly, we need to be able to test those plans.

Many organizations reported a rise in fraudulent transactions following the events, especially activities that fall under money laundering. What are some of the associated risks that organizations need to consider in a time of disaster?

In a time of disaster, we tend to go use facilities that are not as case-hardened and not as protected as those that are in our normal day-to-day operations. So, one of the things we need to make sure of is that the security of those facilities, including Cloud technology, is equal to if not better than our own security. And we have to have some oversight. One of the things we often miss is not having audit/compliance teams available to understand what's going on. In a crisis, we can expect that people will try to commit fraudulent acts, and we have to be prepared for those things.

In your opinion what can be the ideal driver for adopting a culture of BC/DR in a region like the ME where there are no regulations or laws?

Well, one thing is that we are starting to see some of that come about. I think that if you look at the central bank of any Middle Eastern country, you will see that BC/DR is included. But I think the driver is going to be what it has always been, and that is business – outside corporations considering doing business in the Middle East and using Middle East suppliers. Those suppliers are going to have to reach a level that is at least equal to what people are seeing domestically. I think the driver will be business, but I think corporations have shown that they will comply with regulations no matter where they are. And what we've found is if you want to continue to grow your business, you're going to have to have business continuity.

Why you should attend Cairo Security Camp 2011?

First Organized by an Arab Country

Cairo Security Camp is an annual event targeting the Information Security Community of the Middle East and North Africa (MENA Region). IT professionals and security practitioners from throughout the region are invited to attend. Cairo Security Camp is the first Information Security Conference organized by an Arab Country.

Could the cloud save your business from a disaster?

By Mahmoud Tawfik

Cloud Computing has become a significant technology trend and many experts expect that cloud computing will reshape information technology (IT).

According to Forrester's recent survey of 2,803 IT decision-makers, improving Business Continuity and Disaster Recovery (BC/DR) capabilities is the No. 1 priority for SMBs and the second highest priority for enterprises for the next 12 months.

The scope of BC/DR programs is growing also: mature programs address all sources of downtime — including mundane power outages and weather-related disruptions, not just rare, catastrophic disasters. Security and risk professionals should take advantage of this increased visibility as the economic recovery slowly thaws IT budgets to improve the BC/DR's organizational and process maturity for the long term.
The report "Business Continuity and Disaster Recovery Are Top IT Priorities for 2010 and 2011" indicated that 32 % of enterprises and 36 % of SMBs plan to increase spending on business continuity by at least five percent. Only 11 % of enterprises and 8 % of SMBs plan to decrease their spending.

These statistics indicate that businesses are looking for reliability.

The Cloud infrastructure represents a paradigm shift for BC/DR. Businesses are looking for cost-effective solutions for reliability, and a well-designed Cloud Computing architecture with multiple redundant sites makes it suitable for utilization in a comprehensive Business Continuity and Disaster Recovery strategy.

In October of 2010 Aberdeen group surveyed over 100 organizations with formal Disaster Recovery programs to learn whether they used public Cloud storage and if so, what benefits were realized in their performance. Aberdeen discovered that organizations that had moved at least part of their data storage to the Cloud recovered from downtime events almost 4 times faster than those with no formal Cloud storage program. In addition, users of Cloud storage met their Recovery Time Objectives (RTO) more often than those storing their data in-house.

A Cloud-based BC/DR solution is a good fit for any business with a low tolerance for downtime and data loss but this does not guarantee that there are no service outages. For example, a rare and major outage of Amazon's Cloud-based Web service in April took down a plethora of other online sites, including Reddit, HootSuite, Foursquare and Quora.

The main concerns of Cloud Computing are security and privacy issues, which have been further categorized to include sensitive data access, data segregation, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy.
Solutions to various Cloud security issues include greater use of cryptography, particularly public key

Why you should attend Cairo Security Camp 2011?

Eductaion & Knowledge

Sharing Information and knowledge transfer is the main target of Cairo Security Camp 2011
Cairo Security Camp 2011 will include two days of keynote addresses, presentations, panel discussions and more, to an expected combined audience of more than 500 participants
One day will cover the technical topics and the other day will cover the managerial topics

infrastructure (PKI), use of multiple Cloud providers, standardization of APIs, improving virtual machines support and legal support.

The Egypt Cloud Forum organized Egypt Cloud Day to increase the awareness of Cloud Computing and related security issues. The Egypt Cloud Forum is the official affiliate to the Cloud Security Alliance, Egypt Chapter, with the focus area on “Cloud Vulnerabilities Identification and Virtualization Security”.

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best-practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

Egypt CLOUD FORUM

About the author:

Mahmoud Tawfik

I am the CEO of Fixed Solutions and Penetration testing Director at Cloud Security Alliance - Egypt Chapter.

MSTawfik

Email : m.tawfik@fixed-solutions.comg

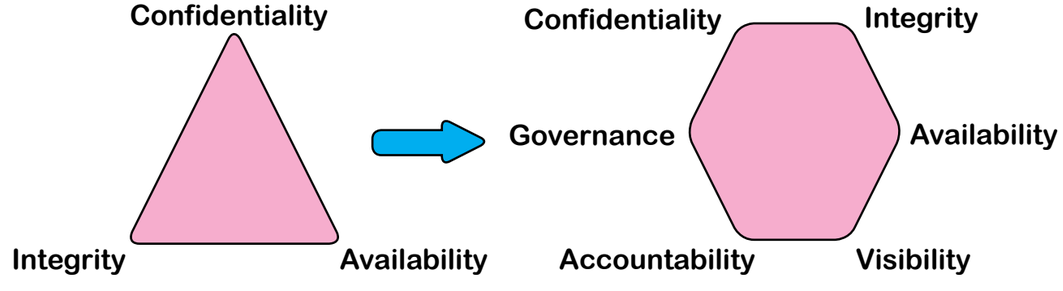
Sources :

http://money.cnn.com/2011/04/21/technology/amazon_server_outage/index.htm
http://www.forrester.com/rb/Research/business_continuity_and_disaster_recovery_are_top/q/id/57818/t/2
http://www.cloudsecurityalliance.org
http://www.egyptcloudforum.com/?q=node/42
http://www.aberdeen.com/aberdeen-library/6827/RA-disaster-recovery-cloud.aspx
http://www.aberdeen.com/aberdeen-library/6827/RA-disaster-recovery-cloud.aspx

Futuristic Approach to Ensuring Data Security in Clouds

By Vinoth Sivasubramanian & Mohamed Mohieldeen

Information Technology has come a long way ever since computers were invented. Similarly Information Security has come a long way. Trends such as Cloud Computing have been helping Small and Medium Investors and Innovators (SMIs) by reducing the initial cost of deployment and maintenance. This will definitely pave a new path ahead for many people. With emerging trends such as these data security in the Clouds must not be viewed in the traditional triadic way but must be viewed in a different way. This paper will discuss ways on how data security paradigms can change in the near future and ways to address the new. Traditionally Information Security has been governed by the “CIA” triad, namely Confidentiality, Integrity and Availability, but this is bound to change in the future especially with data being spread across the globe. This model will ensure a considerably high level of data security and authenticity:



Since there are enough materials and resources available already to address the first three parameters such as Confidentiality, Integrity and Availability we will focus on the other three parameters namely Visibility, Accountability and Governance. We will focus this article from a Process and Governance perspective.

A clear well-defined Service Level Agreement (SLA) is the first step in ensuring the security of our data. Here we provide some fresh approaches to drafting an SLA that will deliver a win-win situation.

1. Accountability:

Accountability is a concept in Ethics and Governance with several meanings. It is often used synonymously with concepts such as responsibility and answerability. From a modern management perspective it can be coined in two words “Stupendous leadership” , this can be looked at from either a people perspective or from an organizational perspective ,wherein both the people and the organization go beyond the call of their duty to create sustaining and winning relationships. Here are some factors that can be woven into the Service Level Agreement:

1.1 Availability:

Draft SLAs which will clearly enlist the minimum time that the organization can hold on disruptions. This is because certain applications in an organization will not be critical as compared to their front-line applications. This way the customer ends up getting better quality of service for their most critical applications. A sample template is given below which can be used as a cue:

Name of Application	Availability Required	Mean Down Time
Internet Banking	100	Nil
HRMS Application	99	1 Hour

1.2 Rewards Management :

This is something new, draft agreements that clearly state the rewards that you will share with the provider if the ultimate goal of providing secure and reliable data quality is met; make them understand the metrics that you require for sharing incentives. Also provide certificate-of-excellence rewards to the people who maintain your infrastructure and help achieve business excellence.

1.3 Loss of business:

Clearly state the legal and other risks that the vendor will incur if they do not meet the metrics that are deemed fit by the organization; outcomes could range from cancellation of contracts to fines imposed due to legal obligations.

1.4 People Employment:

Clearly enlist the kind of people who must be employed to manage your data and infrastructure, the kind of checks that must be done on those people, the credentials (degrees and certifications) that they must hold.

1.5 Good Governance Practices:

Ensure that an organization such as an Internet Service Provider (ISP) will practice good governance principles in reference to management, which is basically corporate governance that extends beyond IT governance. Conducts of good governance guides are available in the OCEG Red book. Organizations that practice good governance are more sustainable in the long term. To cite an example, in the case of an Internet Service Provider going in for a merger or acquisition the ISP should ensure that customers are properly informed and have visibility on what is happening to their data.

1.6 Good IT practices:

Make them accountable to follow good IT practices such as ITIL, SAS70, etc. This will ensure that your data is taken care of properly, as organizations that have these certifications get audited by an independent body. If this is not feasible, get them to follow at the least good Incident Management, Change Management, Release Management, Problem Management and Security Management procedures as per ITIL or any other leading standards. This will ensure confidence amongst stakeholders as well as management.

2. Visibility:

One of the biggest challenges of Cloud Computing is gaining visibility into the infrastructure of the service provider. Most organizations will provide some sort of certification such as ISO 27001 but does that ensure that everything is taken care of? Unfortunately it does not. So how should an organization tackle visibility? Here are certain steps to do so:

2.1 Have a dedicated team in-house:

Have a small but dedicated in-house team of system admins, network admins, or security personnel who can mark the nature of data as to whether it is critical/semi-critical/normal and also monitor the movement of data. The KRA of this team should be to report violations and Log anomalies.

2.2 Implement CCTV Monitoring:

Through CCTV monitoring the customer can have a ground view on the physical security of the place in which the data resides. Record the findings, review them every month, note observations, circulate the observations and archive them on an external storage. These findings will be particularly useful when dealing with legal issues arising out of operations occurring across the globe.

2.3 Identity Management and Access Control:

Ensure that the service provider gives you the power to enforce Identity Management and Access Control privileges as per your requirements; for critical systems implement dual identity authentication wherein changes on require the acknowledgement of two people. Implement Authentication, Authorization, and Audit (AAA) for these systems and have them logged on a sys-log server.

2.4 Backup:

Business Continuity and Disaster Recovery are critical components of availability but the CIO needs to ensure that they have first-hand facts on the back-up data, as to where it is located, who has access to it, and how the data is being managed.

2.5 Implement Logging Server:

Implement a logging server wherein all transactions carried on your infrastructure and data will be logged to this server. Provide no service provider access to this server; access to this server must rest with a specific group of people from within the organization, such as the CISO or CIO only. Ensure that the log files are read-only.

3. Governance:

This pillar is based on the paradigm trust-but-verify. In spite of getting all the above factors correct the CISO or CIO must adopt an audit-based approach. We present a multi-pronged governance approach here.

3.1 Risk Management:

Have a quarterly risk assessment conducted by your internal security team in line with international standards such as NIST or COBIT. Record the observations and have them circulated.

3.2 Vulnerability Analysis and Penetration Testing:

Have a VA/PT done by your internal team every half year and a yearly VA/PT done by a team of external specialists; this will help uncover surprise items and mitigate risks.

3.3 Internal Audit:

Have a year-end audit conducted by an internal team and a similar audit done by external auditors, who are specialists. Have the audits collated, and discuss the results with the top management of service providers. Identify concerns and areas for improvements and have them addressed through various compensating mechanisms.

Conclusion: Cloud Computing is here to stay and will change the way data is being managed, stored and processed. By following the procedures laid out above the CISO/CIO can ensure that a high level of data security can be achieved. The above process requires well-planned strategy, budget and resources but going by the Return-On-Investment (ROI) that Cloud Computing provides management will hardly say NO.

About the authors:

Vinoth Sivasubramanian

Professional security expert focussing to reach pinnacle of excellence in areas of IT security , governance , Ethics and Leadership.

Mohamed Mohieldeen

I am the Vice President Service Delivery and Strategy of Intrendz Consulting

Mail : peermohamed.mohideen@intrendz.co.in

Reference: www.wikipedia.org

secureninja.com
Forging IT Security Experts

Secure Ninja provides expert Information Security training, certification & services.
Visit our Digital Dojo at secureninja.com to see if you qualify or call us at 703.535.8600.

CISSP | CEH v7 | CCNA | CISM | Security + | CAP | CISA | CHFI | ECSA | ISSEP | ISSAP | ISSMP | ECSA | Network+ | EDRP | ECSP