Department of Computer Applications
School of Computer Sciences
Chitkara University, Punjab Campus

CHITKARA UNIVERSITY

August 2013, Volume 1, No. 1

Contents

Contact Information

Dr. Jaiteg Singh

jaiteg.singh@chitkara.edu.in

Mr. Preetinder Singh Brar

preetinder.brar@chitkara.edu.in

Mr. Vikas Rattan

vikas.rattan@chitkara.edu.in

MESSAGE

I'm proud to be a part of Chitkara dynasty. I feel honoured and obliged to the almighty for this valuable present. With the publication of the magazine "Wall for all" which is an applaudable event, the team has proved its love and faith in the department. Chitkara has nurtured number of students with supreme excellence be it academic or co-curricular level. The co-ordinated effort of the faculty has made this department soar great heights. Chitkarians stand apart the crowd and are well recognized. The Chitkarians have proved with their ability, capability, strength and intellect to be recognized globally. Throughout its journey from a pebble stone to the hill mountain, this department has tried to shake hands with the nature. Our efforts have been benefiting from technology but not keeping environment at stake. we at Chitkara have derived pros of technology and hence are better connected and better informed by letting us travel the globe without leaving the desk. And thus, utilizing the power of knowledge, technology and wisdom, Chitkarians tend to enhance themselves in every aspect and move forward with the goal of stop not till the goal is achieved, so their potential can be explored to the core. The potential which will lead them to heights, greater heights.

Dr. (Mrs.) Madhu Chitkara
Vice-Chancellor
Chitkara University

MESSAGE

Department of Computer Application is always a leader in implementing new ideas which benefits its students & faculty. “Wall for all" is another milestone in this context. This departmental e—magazine is initiated by keeping in mind the contribution of students & the faculty members of the department. As new technologies are emerging day by day and everyone can't be aware of each emerging technology, so this e—magazine is a step taken to provide all necessary and important information to the concerned pupils. I would like to thank Chitkara University & all the faculty members who took initiative to launch this magazine.

Mr.Vikram Mangla
Deputy Dean
Department of Computer Applications
Chitkara University

Cloud-based Security

Over the past few years, online attacks have evolved from rogue hackers committing random exploits to targeted, criminal acts. Malicious malware is growing exponentially, causing a dramatic rise in Internet crime. According to a study by the Organization for Economic Cooperation and Development (OECD) concerning online crime, which was released last summer, an estimated one-in-four U.S. computers are infected with malware.

In addition to malware, Distributed Denial of Service (DDoS) attacks are bringing mission-critical systems and business operations to a halt, losing revenue opportunities, decreasing productivity and damaging business reputations. Over the past few years, DDoS attacks have grown in frequency and are conducted for a specific purpose such as extortion, market manipulation and cyberterrorism.

Large-scale data breaches are also becoming prevalent. The breach occurred when cybercriminals planted a keystroke logger onto the company's credit card processing system to pull off 130 million account records affecting at least 160 banks in the U.S., Canada, Guam and elsewhere. Cybercriminals will continue to target processing companies, like Heartland, due to the value of the data they manage. Companies that fall victim to these attacks suffer in a variety of ways. Clean-up is extremely complex and costly —more so to small- and medium-sized businesses. Some smaller companies may entirely lack the appropriate resources to handle the problem in-house. Companies without a large IT department are particularly burdened as the IT team usually consists of a few technology generalists, at most. In these companies, IT personnel wear multiple hats, each possessing a passing knowledge about a variety of topics, and are almost always pressed for time. Security is not a core competency for these organizations, so a different approach is needed to address the growing severity of security issues without draining the entire IT budget and without diverting resources away from running the business. In addition to cleanup costs, companies suffer when they fail to comply with regulatory requirements. At this juncture, only left solution is cloud security.

Exploring Cloud-based Security

Just as appliances became an established security solution 10 years ago, the Internet cloud is now emerging as an up-and-coming platform. According to Gartner, "cloud computing is a style of computing where massively scalable IT-related capabilities are provided 'as a service' using Internet technologies to extend to multiple external customers." Gartner also indicates promise in the computing model and says security applications delivered as cloud-based services will have a dramatic impact on the industry, as cloud-based services' share of the messaging security market will triple by 2013.

Whereas solutions such as the CRM platform, SalesForce.com, clearly fit into the category of Software-as-a-Service (SaaS), cloud-based security solutions are more accurately described as Infrastructure-as-a-Service (IaaS). This distinction is critical to understanding the benefits of cloud-based solutions. With IaaS, the responsibility for managing and maintaining infrastructure lies with the service provider, not the customer's IT staff.

An additional consideration in evaluating cloud-based solutions is the buzz over the safety of cloud-based solutions in general. For example, a Burton Group recently released a report claiming that Amazon's cloud computing service should not be used for applications that require advanced security and availability. Amazon has helped define the cloud computing market space by introducing its Elastic Compute Cloud (EC2), a service offering access to virtual server capacity over the web. There are many advantages to EC2, but security remains a key concern of outside analysts. Although Amazon appears to do a good job of network and physical security, overall the Burton Group awarded the company "low marks for enterprise availability and security" due to a lack of transparency and gave Amazon high marks for scalability and said it offers adequate performance and load balancing capabilities

Weighing the Cloud-based Solution versus Premise-based solution

Several key factors should be considered when deciding between premised-based vs. cloud-based security. The first consideration, of course, is whether an organization is open to the concept of outsourcing. In some industries, such as financial services, outsourcing security may pose risks that outweigh the financial and staffing benefits of a cloud-based solution. In other situations, a company may fear they are relinquishing too much security responsibility to an outside vendor. This, however, is usually untrue. Tasks and responsibilities are frequently shared between the security provider and customer's IT teams to keep all parties fully in the loop.

An additional important consideration is whether an organization's IT staff possesses sufficient expertise and time to manage a premise-based solution. In larger organizations, dedicated security staff may be able to fill this void. In small- to medium-sized organizations, the appropriate skill sets are often lacking. Additionally, smaller staffs mean that resources are usually stretched thin. In this case, cloud-based computing may make sense as the company can benefit from the expertise of a service provider's fully dedicated security team. The service provider is also typically well-versed in serving a customer's needs, unlike premise-based software vendors that may only provide support during an upgrade.

The advantage of a cloud-based proxy model is that capacity can be added as needed. For example, a company may pay for 100 users the first month, 300 the next month and so on. Payment is made when capacity is purchased, replacing a capital expense with an operating expense. In this way too, a company does not have to buy or maintain equipment that will not be used for some time. Additionally, a company turns over the management, maintenance and monitoring to a service provider for additional cost savings. A large company with many users, however, may still prefer a premise-based solution — especially if they already have the personnel on staff to manage it.

Premise-based solutions require physical installation and configuration changes at various points in the network infrastructure while cloud-based solutions require no installation process. Security capabilities are forward-deployed so functions are carried out before traffic even reaches the network.

Financial Considerations

Organizations must also consider financial concerns. Premise-based solutions require investments in infrastructure—network devices, hardware, storage and more. In addition to

capital costs, organizations face staffing concerns as the solutions often require 24X7X365 monitoring. There are also additional, incremental costs for backup, as well as for utilities and rack space.

Although a large company might easily absorb these expenses, smaller companies have a difficult time raising capital and training and paying the necessary IT staff to manage the solution. Cloud-based security solutions eliminate the capital expenditures required for premise-based solutions and, instead, charge a monthly subscription fee. Although some small-to medium-sized companies may find that several years of subscription fees may exceed the cost of a premise-based product and associated support, cloud-security is still usually the more affordable option when factoring in staffing and additional costs. For periods longer than three years, organizations must also consider product replacement costs as well, which could negate any potential benefits to be realized from longer amortization periods.

The Downside to Cloud-based Security

There are several caveats to choosing cloud-based security options. For example, certain solutions are simply more effective if deployed inside the network, such as intrusion detection and prevention systems, application firewalls and data encryption. In the case of data encryption, data must be encrypted before it leaves the network so a cloud-based solution is obviously inappropriate. Also, if an organization expresses serious reservations about outsourcing security functions, security from the cloud will be considered high risk amongst company decision makers — no matter how compelling the financial or customer service considerations are. In addition, cloud based solutions may be deemed too constraining where significant customization is required to suit a particular company's needs.

Some companies also worry about the degree to which customers' data is protected when cloud-based solutions are used. However, cloud-based security solutions do not store business data, but rather, store logs of events that occur within individual security solutions. Questions have also been raised about the identity management mechanisms used to validate users in business applications. Cloud-based security solutions, however, do not hold user accounts linked to a company's business users and, under most circumstances, this data is completely transparent to users.

Call for Articles

At Chitkara University, the endeavor has been to hone the skills of the learners. Keeping in line with this tradition, a magazine titled ***Wall For All*** was proposed. The maiden edition of the magazine has been compiled solely by the core team of ***Wall For All***. However, the students as well as faculty members are encouraged to contribute certain articles of interest for the magazine. The articles must be original in nature, and if adapted, due credit must be extended towards that source.

IT DISASTER RECOVERY

One of the widely used terms in the IT sector is Disaster, and so is Disaster Recovery. Disaster Recovery (DR) refers to the process, policies and procedures that are related to preparing for recovery of infrastructure when a natural or man-made disaster has occurred. This article intends to bring forth the importance of Disaster Recovery, and also the various procedures that the IT companies follow in the event of any disaster.

History

It was in 1970s that the IT managers observed that the organizations were getting more and more dependent on their computer systems. Those were the days when systems were primarily batch-oriented mainframes. In case something went wrong with the system, it was common feature to have the system being down for many days in a row, and that would often result in substantial damage to the organization.

With time, the organizations started to depend more and more on the computer systems. At this point of time, the managers felt the need to handle disasters, and this led to establishment of a completely new industry that specialized in provide data backup through their computer facilities. Moreover, the government regulations were also being brought into force that made it mandatory for the organizations to establish disaster recovery plans. Later on, with the advent of internet, and its being adopted extensively by the business houses, the dependence on IT became even more pronounced. The organizations were now more inclined towards setting a benchmark of making the critical information available for 99.99% of the time. This further proved to be a catalyst for growth of industry that provided disaster recovery services

Importance of Disaster Recovery Planning

With more and more number of companies becoming increasingly dependent on IT systems, it has become prudent to ensure uninterrupted operations of such systems. In the event of any failure of hardware or software, such systems must ensure speedy recovery, without loss of any critical data. Experts dealing with IT disasters strongly advocate the sense of seriousness on the part of the IT companies towards preparation of continuation or recovery of systems. A study conducted by one of the prominent organizations suggests that out of many companies that suffered a major loss of business data, 43% never reopen and 29% close within two years of suffering data loss. Such outcomes of poorly managed IT systems have proved to be eye-openers for other companies, which are ready to spend substantial time and money to ensure that they do not suffer any loss of data in case any disastrous event occurs.

Control Measures

Disaster Control measures are mechanisms that are often put to place by organizations to alleviate, or preferably totally eliminate, the impact of disasters, whether natural or man-made. Various types of methods can be integrated in disaster recovery plan (DRP).

Disaster recovery plan is a subset of a larger process known as business continuity plan. It often includes a plan for resuming the applications, data, hardware, electronic communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes plan for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection. A BCP should refer to the DRP for IT

related infrastructure recovery or continuation. The control measures for IT disaster recovery are classified into the following three types:

1. Preventive measures - Preventing an event from occurring.
2. Detective measures - Detecting or discovering unwanted events.
3. Corrective measures - Correcting or restoring the system after a disaster or an event.

It is worth noting that all good disaster recovery plans advocate the need for all these three types of controls to be documented and tested regularly.

Strategies

Data loss is extremely critical, often requiring extensive planning. Many organizations rely on disaster recovery companies such as SunGard, Comdisco and Recall, which offer office space, computers, and telecommunications equipment when disasters occur. "Cold site" recovery requires the companies to back up their own data onto tapes, storing them offsite. If a disaster occurs, the organizations transport their backup tapes to the recovery sites where they load and boot their applications from scratch using their backup tapes. Although the cold site approach is relatively inexpensive, restoring data can be slow, often taking from a few hours to a week. If the tapes are stored at the affected site or relatively close by, all data may be permanently lost, which could put some companies out of business. Moreover the data for all activity since the last backup will be lost.

"Hot site" backups can solve some problems, but it could cost some companies as much as $1 million monthly. A hot site is located offsite where a reserve computer continually creates a mirror image of the production computer's data. In case a data disaster occurs, the company can quickly switch over to the backup computer and continue to operate. If the primary site itself is destroyed, the staff will actually go to the hot site to operate.

Some of the most common strategies for data protection are

1. backups made to tape and sent off-site at regular intervals (cold site)
2. backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk. (cold site)
3. replication of data to an off-site location, which overcomes the need to restore the data (only the systems then need to be restored or synchronized), often making use of storage area network (SAN) technology (hot site)
4. the use of high availability systems which keep both the data and system replicated off-site, enabling continuous access to systems and data, even after a disaster. (hot site)

In many cases, an organization may elect to use an outsourced disaster recovery provider to provide a stand-by site and systems rather than using their own remote facilities, increasingly via cloud computing.

In addition to preparing for the need to recover systems, organizations also implement precautionary measures with the objective of preventing a disaster in the first place. These may include

1. local mirrors of systems and/or data and use of disk protection technology such as RAID
2. surge protectors - to minimize the effect of power surges on delicate electronic equipment
3. use of an uninterruptible power supply (UPS) and/or backup generator to keep systems going in the event of a power failure
4. fire prevention/mitigation systems such as alarms and fire extinguishers
5. anti-virus software and other security measures.

Real World Story

Morgan Stanley resumes ***Business-Critical*** Operations Within Minutes of **Attack on World Trade Centre**.

It was on September 11, 2001, when four passenger jetliners were hijacked in the USA. One was crashed into a section of the Pentagon, another plunged into the Pennsylvania countryside when passengers prevented the hijackers from hitting their target. The other two planes were crashed into New York City's two World Trade Center (WTC) towers that killed thousands of people.

All WTC offices were destroyed, majority of which comprised of financial companies. The financial industry's equipment loss was immense. Much of the WTC IT and telecommunications equipment was located underground and had been destroyed by the collapsed debris. It was estimated that over 16,000 trading-desk workstations, 34,000 PCs, 8,000 servers, plus large numbers of information computer terminals, printers, storage devices, and network hubs and switches had been damaged due to the collapse of WTC.

While many companies lost a lot of data in the attack, a Morgan Stanley's WTC facility was probably one of the best-prepared from a systems and data recovery perspective. Lower Manhattan's extraordinary data security concern erupted in 1993 when a large bomb exploded in the subterranean parking area of the WTC in a terrorist attack. Realizing the vulnerability, many companies initiated steps to protect themselves, and Morgan Stanley was one of them.

The company had contracted with a prominent disaster recovery company for "hot site" disaster recovery. Although Morgan Stanley never hoped to use this site in future, yet it went on to pay millions of dollars annually for maintenance of cold sites. Data was maintained not only at the primary location the company, but also at the recovery sites. After the attack on WTC, Morgan Stanley shifted its employees to Brooklyn and Harborside where the employees took over the terminals at the recovery sites. Morgan Stanley's distributed technology platform and voice systems at the World Trade Center facility were destroyed and had to be rebuilt at recovery locations. At the same time, up to 80 percent of inbound phone traffic to Manhattan (the WTC location) was blocked. The Morgan Stanley Telecommunications Group rerouted some of the traffic to internal facilities and through the Tokyo office to thwart the problem. The firm's secondary and tertiary connectivity for overseas circuits also provided enough capacity to handle over 100 percent of peak load demand.

To a remarkable degree, Morgan Stanley stayed in business throughout that first day and during the recovery. Sales personnel contacted clients, despite market stoppages. Retail branch offices were open on Saturday, September 15 to allow clients to reach their financial advisors before Monday's market reopenings. The Equity Research division published a special industry impact report just two days after the attacks.

References

http://en.wikipedia.org/wiki/Disaster_Recovery

http://wps.prenhall.com/bp_laudon_essmis_6/21/5556/1422339.cw/content/index.html

Common Interview Questions for Computer Science Majors

Interviewing with companies for software engineering positions, whether large or small, have a variety of approaches and timelines in the hiring process. Generally speaking, larger companies have a more formal interview process involving a selection committee who conducts phone interviews, having a video web chat online, and one or more site visits. Smaller companies may have a more streamlined approach resulting in a quick phone interview with their recruiter followed by an interview on site. Most of the questions you will be asked are geared towards your technological proficiency. Some will be inquiring about your personality and teamwork skills.

Examples:

- Please tell me about yourself.
- What makes you interested in this position?
- What do you know about our organization?
- What do you consider your greatest strengths?
- What would former coworkers/professors/supervisors say about you if we called them as a reference?
- Why did you choose this field?
- How did your college experience prepare you for a career in this field?
- Describe the work environment that makes you thrive.

More Examples:

- If you have ever dealt with difficult people, how did you manage conflict?
- What are your proven coping mechanisms in challenging times?
- If creative, where you do get your inspiration?
- Convince me you are the perfect match for our opening.
- What sort of pay do you expect to receive?
- How does your previous experience relate to the job we have open?
- How did you get along with your last boss?
- What is the hardest job you have ever held?
- Do you have any questions for us?

Top 10 Things to Consider for the Interview

1. An interview is a conversation about what you can do for them; research the company and tailor your responses towards substantiating how your talents and personality match the position.
2. Rehearse interview questions out loud with a friend, family member, or your Career Advisor.
3. Arrive at least 15 minutes early, but enter the premises 8-10 minutes early.
4. Bring copies of your resume and reference sheet with you to offer.
5. Use professional language and avoid slang words such as "uh," "um," "you know," and "like."
6. Body language should be professional: good posture, not slouched, good eye contact but not staring. Watch the nervous habits of twirling hair, tapping a foot, or drumming fingers.
7. Smile, it'll help you … and then … relax!
8. Be prepared to offer evidence through detailed examples of times and ways and situations you used certain technical applications, characteristics, or skills.
9. Collect their business cards so you can follow up with a thank you card or e-mail.
10. After the interview, take notes on everything you can remember and use the experience to further develop your interview techniques.

Questions to Consider Asking the Interviewer

Adapted from "Three Questions to Ask" by Toni Bowers, 2009

So many people are concerned with making a good impression during a job interview that they forget it's a two-way street. You're there not only to market yourself but to find out if the job and the company are a good fit for you. You should use the interview to ask questions for yourself. So what type of questions should you be asking? Here are a few.

1. What's an average day like here?

The question may prompt the interviewer to go into great detail about the day-to-day workings of the company, which is great information to have. If you deem it appropriate, respond to their answer with an example of how their work environment suits your style of operation.

2. How would you describe the culture here?

The interviewer may answer that it's pretty laid-back or it's all business, or there's a good mixture of gender and cultures. Of course, he may also lie through his teeth. But if you're any good at reading people, even that might be valuable.

3. **What qualities are you looking for in the person who fills this position?**

You're looking for answers like "Someone who is good with details" or "Someone who can communicate technical issues to end-users," etc. If the answer is "Someone who doesn't mind skipping lunch or always being on call," then you have some solid information on which to base your decision about the job.

Other Questions to Consider Asking:

1. What is the next step in the hiring process? Or, when might you make a hiring decision?
2. What tools/applications/languages do you use?
3. What is your history with student interns/employees?
4. What typical projects or tasks do student interns work on?
5. What makes a student intern successful? What trade is best suited for your company?
6. How do the various member of the team work together-who is in charge? Etc.
7. How would successful performance in this position we measured?
8. Is there much turnover in your company?
9. What's the management style?
10. Do entry dash level employees get to travel to conferences? Is that a perk or are they on their own?
11. What make new college grads attractive; what should student we work on?

Top 10 Personal Values Employers Seek in Employees:

1. Honesty/Integrity
2. Adaptability/Flexibility
3. Dedication/Tenacity
4. Reliability/Responsibility
5. Loyalty
6. Positive Attitude/Motivation
7. Professionalism
8. Self-Confidence
9. Self-Motivated
10. Willingness to Learn

NEWS FROM INDUSTRY

Samsung Buys Boxee

Media Streaming device Outfit now under Samsung's Wing

Samsung has expanded its portfolio within the technology industry by buying the Israeli media streaming device firm Boxee.

Acquiring key telent and assets from the company, Samsung is looking to improve the user experience right across its connected devices. Boxee is known for producing devices that let subscribers record TV shows onto its servers, streaming the to TVs, computers and smart devices from the cloud. Now, all that cloud functionlity comes under Samsung's roof.

In other Samsung news, the firm has forecast weker-than-expected profits for April to June with an estimated operating profit of 5.5 billion pounds (9.5 trillion South Koren won). Analysts had expected something around 10.1 trillion won figure.

Concerns appear to lie around the company's smartphone performance, with worries that its growth in that area might be slowing, even in the face of new models having been launched. With Samsung in a spot of smartphone bother, can its competitors take advantage?

Computer Mouse Inventor Passes Away

Doug Engelbart revolutionized the way we all use computers. Engelbart invented the computer mouse, developing the device in the 1960s, back then no more than a wooden shell covering a couple of metal wheels. Engelbart patented his invention way before it was picked up for widespread use across the globe and he was something to a tech-head, having worked on early forms of email, word processing and video teleconference technology at a research institute in California.

This visionary of men was to change the face of computing forever, so take a moment to think of him when you scroll down a web page today.

Corporate Office:
Saraswati Kendra
SCO 160-161, Sector 9 C,
Chandigarh 160 009
INDIA

Phones:
+91-172-2746209, 2747057

Fax:
+91-172-2746154

www.chitkara.edu.in
ca.chitkara.edu.in