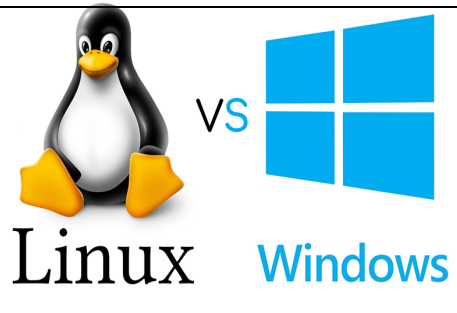
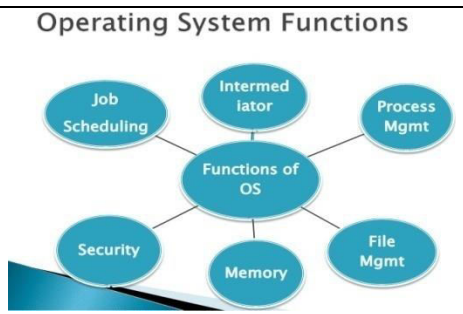
CIT210 OP. SYS. MANAG.

CSUN
COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

Week 11 Day 1: Cloud Security, Major Cloud Outages, Cloud Bankruptcy Concerns, NIST Guidelines on Cloud Security, Cloud Authentication issues, Cloud Security Risks and Countermeasures





Major Cloud Outages

- Nice summary in "The Biggest Cloud Outages
  A couple of examples...
- "AWS, This was the outage that shook the industry.
  An Amazon Web Services engineer trying to debug an S3 storage system in the provider's Virginia data center accidentally typed a command incorrectly, and much of the Internet – including many enterprise platforms like Slack, Quora and Trello – was down for four hours. [...]"
- "Microsoft Azure, Storage availability issues plagued Microsoft's Azure public cloud for more than eight hours, mostly affecting customers in the Eastern U.S. [...] A Microsoft engineering team later identified the culprit as a storage cluster that lost power and became unavailable."

Zeus and Amazon

- In 2009, the Zeus banking Trojan has been spotted using the Amazon service as a C&C (command and control) server.
  - Compromised computers report to EC2 for new instruction and updates.
  - Amazon's Relational Database Service is a backend alternative in case losing access to original domain.
- Crimeware will dive deep into the cloud.
  - Facebook
  - Google App Engine
  - ...

Google Phishing

- In 2011, Google announced that hundreds of Gmail account were compromised in phishing
  - Attackers have enough information to create an e-mail that seems like someone you know.
  - Attackers try to stolen your password and access your e-mail account.
  - Attackers secretly reset settings to copy and forward all e-mails.

Google Phishing (cont.)

- Hackers attack Gmail to stolen the login details
  - Senior US and South Korean government officials
  - Chinese political activists
- Chinese Gmail attack raises cyberwar tensions
  - There is no direct evidence that the hackers were in the pay of the Chinese government.
  - The US government classifies cyber-attacks as acts of war.

Wikileak and Anonymous

- WikiLeaks is an international non-profit organization
  - publishes submissions of private, secret, and classified media.
  - under DDoS attack around the time of an expected release of classified State Department documents.
- WiliLeaks want to move into Amazon EC2
  - EC2 were successfully defended against large-scale DDoS attack.

Wikileak and Anonymous (cont.)

- But in 2011 December, many cloud computing providers stop service for WikiLeaks
  - EveryDNS dropped its domain name service.
  - Amazon took it off its computers.
  - PayPal and MasterCard cancelled its account.
- Anonymous (hacker group) attacks on the opponents of WikiLeaks
  - PayPal and MasterCard are forced to stop online service.
  - But hackers stop attack Amazon because realizing how little impact it was having.

Dropbox Security

- In 2011, Dropbox security glitch meant any password works
  - Everyone can access dropbox if he know the e-mail.
  - Dropbox's authentication is failed in one hour and stop service for up to three hours.
- Dropbox claims that they encrypt user data on client
  - In fact, workflow of encryption is on server.
  - Staff could access the sensitive data.

Dyn, DDoS'd Off The Air

Dyn DDoS attack exposes soft underbelly of the cloud

The DDoS attack against Dyn affected numerous websites, but the biggest victims are the enterprises that rely on SaaS for critical business operations

It's apparently possible that a DDoS attack can be big enough to break the internet -- or, as shown in the attack against ISP Dyn, at least break large parts of it.

The DDoS attack against Dyn that began Friday went far past taking down Dyn's servers. Beyond the big-name outages, organizations could not access important corporate applications or perform critical business operations.

See: https://www.infoworld.com/article/3134023/security/dyn-ddos-attack-exposes-soft-underbelly-of-the-cloud.html

It's Not Just The Network or the DNS: Storage Can Be Key

Cisco loses customer data in Meraki cloud muckup

'Erroneous policy' upload deleted custom apps, IVR menus and custom bling

By Simon Sharwood, APAC Editor 6 Aug 2017 at 23:19 22

Cisco has admitted to a cloud configuration cockup that erased customer data.

The networking giant explained: "On August 3rd, 2017, our engineering team made a configuration change that applied an erroneous policy to our North American object storage service and caused certain data uploaded prior to 11:20AM Pacific time on August 3 to be deleted."

"Our engineering team is working over the weekend to investigate what data we can recover," Cisco's advisory says, adding that the company is working on "tools we can build to help our customers specifically identify what has been lost from their organization."

Source: https://www.theregister.co.uk/2017/08/06/cisco_meraki_data_loss/

Power Issues Continue To Be A Challenge For Enterprise Data Centers As Well As "The Cloud"

Delta Data Center Outage Grounds Hundreds of Flights

Ed Bastian, CEO, Delta Air Lines, in a video apologizing to customers for disruption of travel caused by a data center outage in August

Airline attributes outage to power problem in Atlanta data center

Yevgeniy Sverdlik | Aug 08, 2016

Delta Airlines hasn't yet explained what
Atlanta this morning, which led the carri
the day.

It said a power outage "impacted Delta c
but a spokesman for the utility whose ser
Wall Street Journal that there were no p
or Monday. The utility, Georgia Power, d
help Delta fix a problem with switch gear

Delta: Data Center Outage Cost Us $150M

Travelers wait in line at the Delta check-in counter at LaGuardia Airport , August 8, 2016 in the Queens borough of New York City. Delta flights around the globe were grounded and delayed on Monday morning due to a system outage. (Photo by Drew Angerer/Getty Images)

Price tag extraordinarily high in comparison to data center industry average

Yevgeniy Sverdlik | Sep 08, 2016

The Delta Airlines data center outage that grounded about 2,000 flights over the span of three days in August cost the company $150 million, the airline's representatives told the audience of a transportation industry conference in Boston Wednesday.

http://www.datacenterknowledge.com/archives/2016/09/08/delta-data-center-outage-cost-us-150m

Mitigating Cloud Computing Availability Issues

- Risk analysts will tell you that when you confront a risk, you can try to eliminate the risk, you can mitigate/minimize the impact of the risk, or you can simply accept the risk.
- If you truly require non-stop availability, the normal solution is to add redundancy. It's unlikely that all sites you're using will all be down the same time

Mitigating Cloud Computing Availability Issues

- To help with that, some cloud computing services offer service divided into multiple "regions." By deploying infrastructure in multiple regions, isolation from "single-region-only" events (such as the power outage mentioned previously) can be obtained.
- Sometimes, though, it may simply make financial sense for you to just accept the risk of a rare/brief outage. Remember:
  99.99 availability==> less than an hour of downtime/year;
  99.9 availability==> less than 9 hours of downtime/year)
- *Are you really willing to double your costs to cover 9 hours down?*

How Do We Know That We're Appropriately "Managing" Risk (Assuming We Are)

- ***Professional Expertise*** **("I'm not *detecting* us getting hit, and I'm not *hearing reports* that we've been hit, and I've managed all the security risks I've been able to, so...")**
- ***Historical Reputation:*** **we haven't been hacked previously, so we must be okay ("prior performance doesn't guarantee future...")**

How Do We Know That We're Appropriately "Managing" Risk (Assuming We Are)

- *Expenditures:* we're spending everything we've been able to get for securing things (but what if you've got a security person who's bad at playing organizational "budget war games"?)
- *Audit:* the auditor doesn't return any findings (but what if we've got a crumby auditor who isn't paying attention?)
- *Common Sense Test:* if something bad happens, will what we're currently doing pass the public "sniff test"? That is, are we doing what a reasonable person would normally do?
- Remember: not everything is "mission critical."

"Facebook DOWN: Social network NOT WORKING after massive web and app outage“

[* *] Users have [...] flocked to Facebook's big rival Twitter to report issues with the service this afternoon.*

One user tweeted: "FACEBOOK IS DOWN"

While another said: "OMG! Facebook is DOWN! What do we do? It's a crisis."

And one fan even suggested it was the end of the world saying: "What happened to Facebook!? It's actually DOWN. The apocalypse must be here!! #facebookdown."

http://www.express.co.uk/life-style/science-technology/865161/Facebook-DOWN-not-working-outage-why-log-in

The Ultimate Availability Problem: Bankruptcies

blogs.wsj.com/venturecapital/2013/10/01/nirvanix-files-for-chapter-11-bankruptcy/

October 1, 2013, 6:11 PM

Nirvanix Files for Chapter 11 Bankruptcy

Article | Comments (4)

Email | Print

By DEBORAH GAGE CONNECT

Cloud storage company Nirvanix Inc. on Tuesday filed for Chapter 11 bankruptcy in Delaware federal court, the culmination of a startling flop for what was once seen as a high-flier among cloud startups.

The filing comes on the heels of a notice the company posted on its website last week saying that it was working with International Business Machines Corp. to either return customers' data or help them move it to another cloud storage provider and would try to be available through October 15.

Kharisma Tarigan/Agence France-Presse/Getty Images

Nirvanix had raised more than $70 million in venture capital since its founding in 2007, according to VentureWire records. In May 2012 after the last funding round, which was $25 million, former Chief Executive Scott Genereux told VentureWire that Nirvanix was growing and headed toward profitability and a possible IPO.

Its largest equity holders are Khosla Ventures and TriplePoint Capital, which may

Cloud Bankruptcy Concerns...

- If you prepaid (to lock in prices/get a multiyear discount), is that prepaid money safely in escrow somewhere (and able to be refunded), or is it flat out gone?
- Can you find a replacement provider that will be able to take over when it comes to providing the same service that your former cloud provider delivered? (standardized services offered by multiple providers will obviously be easier to replace than unique or bespoke applications)

Cloud Bankruptcy Concerns...

- If there were custom modifications made to the software you were using, do you have copies of what was changed, and could you replicate them elsewhere?
- Perhaps most critically: can you get your data out, and in format that's usable elsewhere? (Proprietary formats should make the hair on the back of your neck stand up.)

Security Questions

- Before jump into cloud computing, following questions consumer may ask
  - What's the security strategy?
  - How to prove the reliability and security that vendor claimed?
  - Can someone access my data without my permission?
  - Who is responsible for policy distribution, management and control?
  - What are the emergency response measures and compensation mechanisms?

Security Issues of Cloud

- Businesses should perform due diligence on security threats both from outside and inside the cloud
  - Cloud users are responsible for application-level security
  - Cloud vendors are responsible for physical security and some software security
  - Security for intermediate layers of the software stack is shared between users and vendors
- Cloud providers must guard against theft or denial-of-service attacks by their users and users need to be protected from one another
- Businesses should consider the extent to which subscribers are protected against the provider, especially in the area of inadvertent data loss

NIST Guidelines on Cloud Security

NIST SP 800-144:

- Governance
- Compliance
- Trust
- Architecture
- Identify and access management
- Software isolation
- Data protection
- Availability
- Incident response

Compass

- When we invested in the cloud computing
  - How to build the secure cloud environment or platform?
  - How to maintain the cloud service?
  - How to migrate from one cloud vendor to another safely and painless?
- There are many key issues for cloud security
  - Data protection, service quality guarantee, disaster recover …etc.
  - Customers need a guideline to search a secure cloud vendor.
  - Cloud vendor also need a guideline to build a secure cloud environment.

Loss of Direction

- When the cloud companies or customers loss of direction on cloud security
  - They may pay lots of money and resource on the useless efforts.
  - They may pay lots of money and loss the intangible assets on the unsecure cloud services.

Cloud Security and Issues

Cloud models and Issues

- Different deployment models: Private, Public, and Hybrid
- Private: Issue “still have to buy, build, and manage them”
- Public: No direct connection and control. Amazon, Microsoft and Google
- Hybrid : lack the flexibility, security and certainty of in-house applications

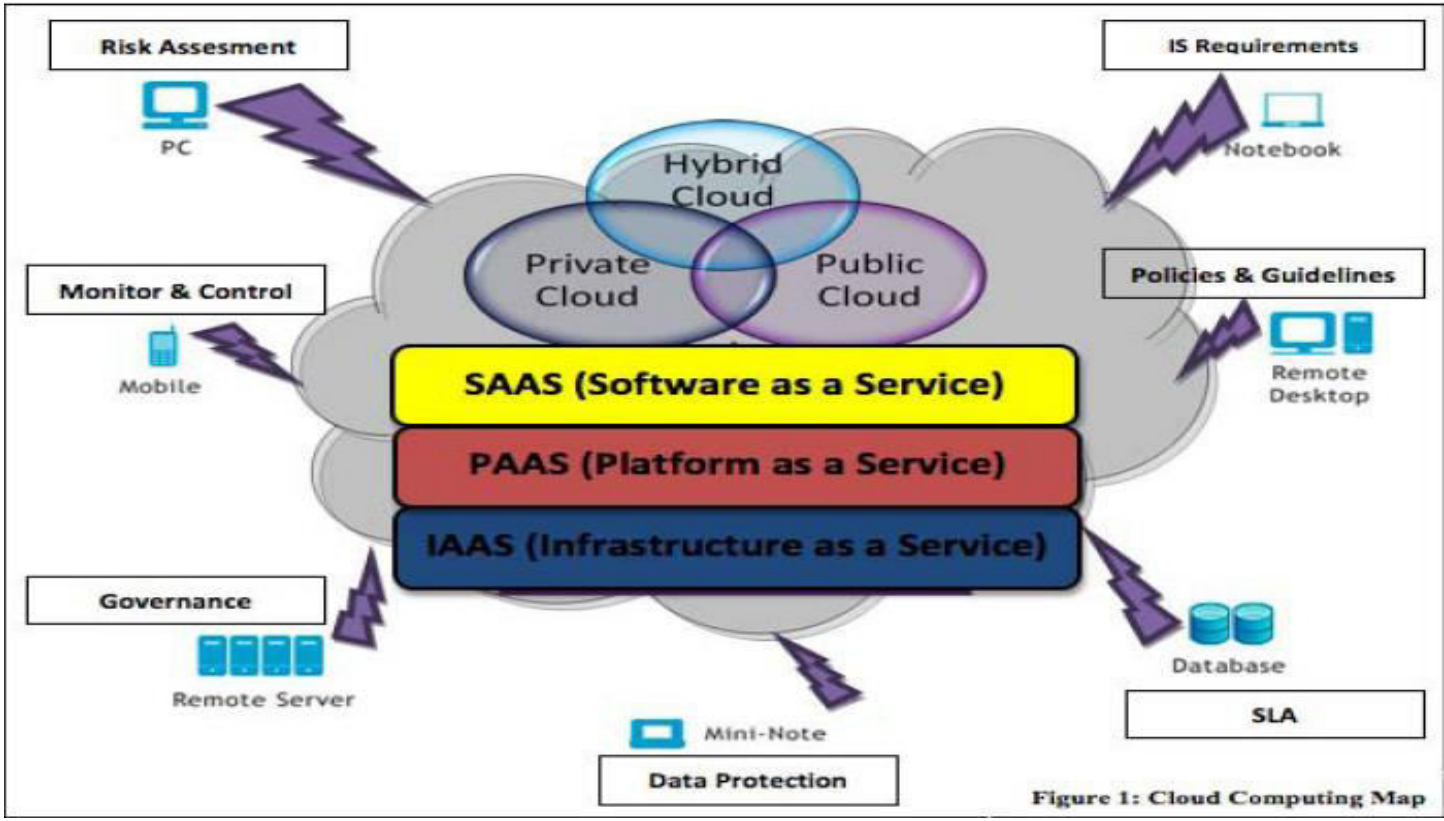
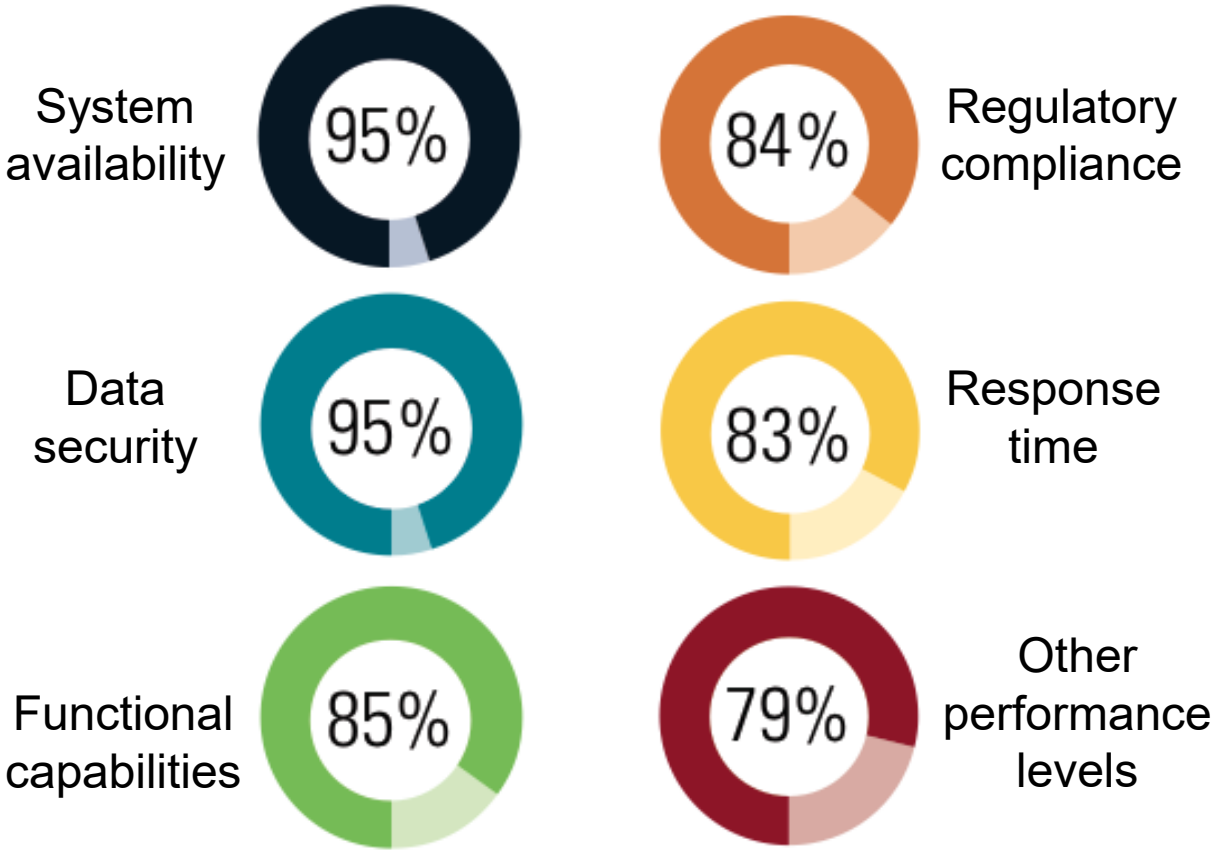


Figure 1: Cloud Computing Map

Top SLA parameters



The most important SLA parameters today?*

Overview of cloud computing security considerations

- Maintaining availability and business functionality
  - My data or functionality to be moved to the cloud is not business critical.
  - I have reviewed the vendor's business continuity and disaster recovery plan.
  - I will maintain an up to date backup copy of my data.
  - My data or business functionality will be replicated with a second vendor.
  - The network connection between me and the vendor's network is adequate.

Overview of cloud computing security considerations

- Maintaining availability and business functionality
  - The Service Level Agreement (SLA) guarantees adequate system availability.
  - Scheduled outages are acceptable both in duration and time of day.
  - Scheduled outages affect the guaranteed percentage of system availability.
  - I would receive adequate compensation for a breach of the SLA or contract.
  - Redundancy mechanisms and offsite backups prevent data corruption or loss.

Overview of cloud computing security considerations

- Maintaining availability and business functionality
  - If I accidentally delete a file or other data, the vendor can quickly restore it.
  - I can increase my use of the vendor's computing resources at short notice.
  - I can easily move my data to another vendor or inhouse.
  - I can easily move my standardized application to another vendor or inhouse.

Overview of cloud computing security considerations

- Protecting data from unauthorized access by a third party
  - My choice of cloud sharing model aligns with my risk tolerance.
  - My data is not too sensitive to store or process in the cloud.
  - I can meet the legislative obligations to protect and manage my data.
  - I know and accept the privacy laws of countries that have access to my data.
  - Strong encryption protects my sensitive data at all times.
  - The vendor suitably sanitizes storage media storing my data at its end of life.

Overview of cloud computing security considerations

- Protecting data from unauthorized access by a third party
  - The vendor securely monitors the computers that store or process my data.
  - I can use my existing tools to monitor my use of the vendor's services.
  - I retain legal ownership of my data.
  - The vendor has a secure gateway environment.
  - The vendor's gateway is certified by an authoritative third party.

Overview of cloud computing security considerations

- Protecting data from unauthorized access by a third party
  - The vendor provides a suitable email content filtering capability.
  - The vendor's security posture is supported by policies and processes.
  - The vendor's security posture is supported by direct technical controls.
  - I can audit the vendor's security or access reputable third party audit reports.
  - The vendor supports the identity and access management system that I use.
  - Users access and store sensitive data only via trusted operating environments.

The difference

- **Internal System**
  - More secure authentication like LDAP, KERBOES
  - Company has a control over the data and process
  - User management is easy and more controlled
- **Cloud System**
  - Proprietary authentication system
  - It is a nightmare to manage the users remotely. We wont know what the vendor is doing
  - Migration is very difficult. It is difficult to synchronize login and authentication data between external clouds and internal systems without exposing internal security data.

Cloud Authentication issues

- Cloud service providers request customers to store their account information in the cloud, cloud service providers have the access to these information. This presents a privacy issue to the customer's privacy information.
- Many SLAs have specified the privacy of the sensitive information, however, it is difficult for customers to make sure the proper rules are enforced. There is a lack of transparency in the cloud that allows the customers to monitor their own privacy information.

Cloud Authentication issues

- When a customer decide to use multiple cloud service, the customer will have to store his/her password in multiple cloud, the more cloud service the customer is subscript to, the more copy of the user's information will be. This is a security issue for the customers and the cloud service providers.

Cloud Authentication issues

- The multiple copies of account will lead to multiple authentication processes. For every cloud service, the customer needs to exchange his/her authentication information. This redundant actions may lead to an exploit of the authentication mechanism.

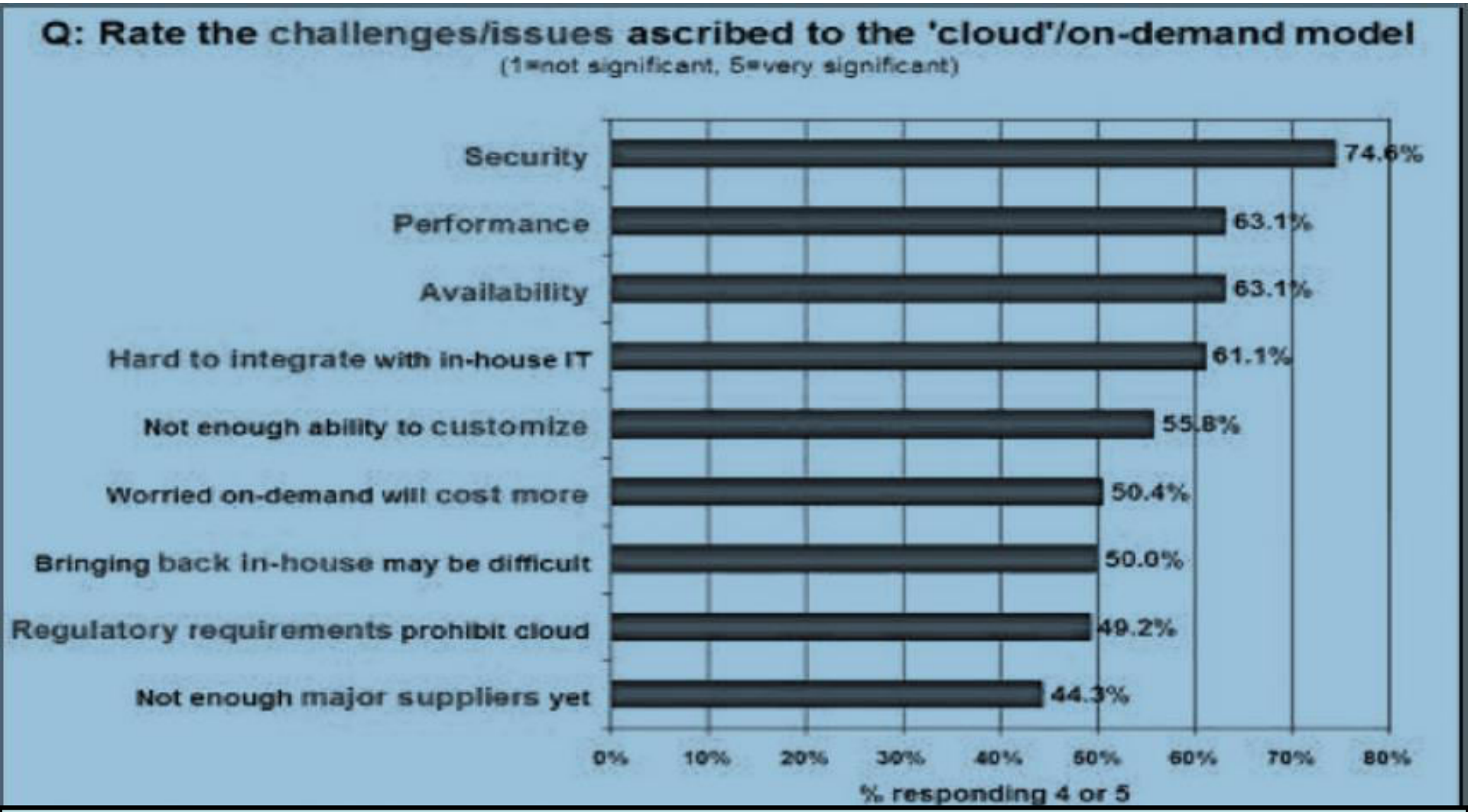
Cloud Authentication issues

- Cloud service providers use different authentication technologies for authenticating users, this may have less impact on SaaS than PaaS and IaaS, but it is present a challenge to the customers.

Authentication issues - contd

- Wells Fargo Customer Data Breached – How Did Cyber-Criminals Get The Access Codes? – Why No Strong Authentication?
  - Dictionary attack?
- Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing as depicted in the chart.

Survey on Cloud computing



Security

- Security is the degree of protection against danger, damage, loss and crime.
  - Security is focused on hardware mechanism, software vulnerability and information hiding.
  - Malicious attackers wants to steal data or destroy system
- Security evolution can be divided into three parts
  - Secure technique
  - Secure management
  - Cyber security

Secure Technique

- **Original security that provides the basic protection mechanism**
  - **Authorization specifies the access right to resource and reject the request from the unknown user.**
  - **Encryption makes information unreadable to anyone except those possessing special knowledge.**
  - **Uninterrupted power supply (UPS) and remote backup server avoid the data lose or server interrupt cause by natural disasters.**

What is access control?

- Access control is the heart of security
- Definitions:
  - *The ability to allow only authorized users, programs or processes system or resource access*
  - *The granting or denying, according to a particular security model, of certain permissions to access a resource*
  - *An entire set of procedures performed by hardware, software and administrators, to monitor access, identify users requesting access, record access attempts, and grant or deny access based on pre-established rules.*

Access Control

- Fundamental function of security is controlling access to critical resources that require protection.
- Access controls can be implemented at various points in a network.
- Access control can be managed in centralized or de-centralized models.

Access Control

- Access Control Implementation Points
  - Network Level- Entire network based on source of request. IP address.
  - Subnet Level- permit or deny based on source or destination.
  - Server Level- Domain user rights, drive share rights, folder/file rights.
  - Device Level- Router, switch, firewall, IDS.

Access Control

- The process of enforcing access right and is based on following three entities
  - Subject
    - is entity that can access an object
  - Object
    - is entity to which access can be controlled
  - Access Right
    - defines the ways in which a subject can access an object.

Access Control Subjects

- Authorized—Those who have presented credentials and have been approved for access to the resource
- Unauthorized—Those who do not possess the proper credentials or do not have the appropriate privileges to access the resource
- Unknown—
  - Those who have not presented any credentials at all; it is unknown whether they should be given access or not unknown person is anonymous.
  - They have not attempted to log in or access a restricted resource—yet.
  - As soon as an unknown person attempts to access a restricted resource,
  - they must fall into one of the other two categories: authorized or unauthorized.

Applying Access Objects

- There are three main categories of objects to be protected by access controls:

- Information—Any type of data asset

- Technology—Applications, systems, and networks

- Physical location—Physical locations such as buildings and rooms

Steps of Access Control Process

Access control requires:

- **Identification**

- **Authentication**

- **Authorization**

Access control process:

- **Subject:** presents credentials to the system
- **Authentication:** system verifies and validates that the credentials are authentic
- **Authorization:** grants permission to allowed resources

Access Control Systems

A well-defined access control system consists of three elements:

- Policies—Rules developed by someone with a strong knowledge of the organization, its assets, goals, and challenges
- Procedures—Nontechnical methods used to enforce policies
- Tools—Technical methods used to enforce policies

Applying Access Objects

- There are three main categories of objects to be protected by access controls:

- Information—Any type of data asset

- Technology—Applications, systems, and networks

- Physical location—Physical locations such as buildings and rooms

Steps of Access Control Process

Access control requires:

- **Identification**

- **Authentication**

- **Authorization**

Access control process:

- **Subject:** presents credentials to the system
- **Authentication:** system verifies and validates that the credentials are authentic
- **Authorization:** grants permission to allowed resources

Authentication Elements

- Password—
  - Secret word or combination of characters that is known only to the subject.
  - A good password is difficult to guess but easy for the subject to remember.
- Token—
  - Something the subject has that no one else does, such as a smart card or a challenge-response device.
- Shared secret—
  - Something only the subject and the authentication system know, such as the name of the subject's favorite pet or the mother's maiden name.

Authentication

- One Time Passwords (Dynamic Passwords)
  - A **one-time password** (**OTP**), also known as **one-time pin** or **dynamic password**, is a password that is valid for only one login session or transaction, on a computer system or other digital device.
  - Used for authentication purposes and are only good once.
  - Can be generated in software (soft tokens), or in a piece of hardware

Authentication (Security Tokens)

- A **security token** is a physical device used to gain access to an electronically restricted resource.
- The token is used in addition to or in place of a password.
- It acts like an electronic key to access something.
  - Examples include a wireless keycard opening a locked door,
  - or in the case of a customer trying to access their bank account online, the use of a bank-provided token can prove that the customer is who they claim to be.

Authentication (Security Tokens)

- Some tokens may store cryptographic keys that may be used to generate a digital signature, or biometric data, such as fingerprint details.
- Some may also store passwords.
- Some designs incorporate tamper resistant packaging, while others may include small keypads to allow entry of a PIN or a simple button to start a generating routine with some display capability to show a generated key number.
- Connected tokens utilize a variety of interfaces including USB, near-field communication (NFC), radio-frequency identification (RFID), or Bluetooth.
- Some tokens have an audio capability designed for vision-impaired people.

Authentication (Security Tokens)

- Two types of Token Devices (Password Generator)
  - Synchronous
    - Synchronous tokens are powered by event triggers or clocks kept in sync with an authentication system.
    - Users generate codes by viewing their tokens at the same time they authenticate themselves or by pressing buttons on certain tokes to generate codes.
    - Time Based
    - Time synchronous authentication refers to a type of Two Factor Authentication (TF-A) method that uses synchronous or time-synchronized tokens for authentication.
    - The server and the token have individual clocks that should be synchronized to the exact same timebase.

Authentication (Security Tokens)

- Two types of Token Devices (Password Generator)
  - Asynchronous
    - Asynchronous tokens are also called Challenge/Response tokens.
    - They do not need event counters or internal clocks to operate.
    - The authentication process sends a challenge — short string of letters/numbers — which the user must enter into the token to generate a response.
    - Know the different types of devices and how they work.

Authentication

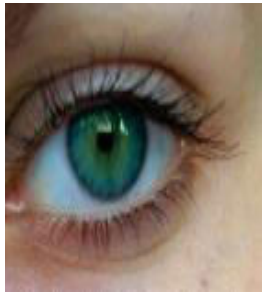
- Hashing & Encryption
  - Hash or encrypting a password to ensure that passwords are not sent in clear text (means extra security)
- Windows environment, know syskey modes.
- Salts: Random values added to encryption process for additional complexity.

Authentication Elements

Authentication elements can be any of the following or a combination of the following elements:

- **Something you know:** password/passphrase, PIN number

- **Something you are:** biometrics, retina, fingerprint, facial


- **Something you have:** tokens, device

Logical Access Controls

- Logical access controls can be based on one or more criteria, including:
- Who—
  - The identity of the subject, proven by a username and password combination
- What—
  - The presence of a specific device or access token
- When—
    - Combined with subject identity, access can be granted during one time period and denied at another time

Logical Access Controls

- Where—
  - Either physical or logical location
  - “Logical location” refers to the Internet Protocol (IP) address or Media Access Control (MAC) address a user connects from.
- Why—
  - The defined purpose for which access must be granted to a subject
- How—
  - What type of access can be granted to a subject
- Administrative—The ability to read, write, create, and delete files
- Author—The right to read and write to his or her own files
- Read only—Can read but not edit files
- No access—Complete denial of access

Objects

- Data element—
  - This is the lowest level of granularity for information-based assets.
  - For example, if a database table contains a Social Security number, you may need to place special restrictions on that data element.

Objects

- Table—
  - You may also define a database table as an object.
  - You could grant users access to tables containing employment information, order information, or other types of information based upon their roles in the organization.

Objects

- Database—
  - You can also define an entire database as an object.
  - For example, you might grant all employees read-only access to the entire product information database, and give product managers write access to certain tables or rows within that database.

Objects

- Application—
  - An application is also an object.
  - You might wish to grant some users the ability to run an application, while denying it to other users.
  - Applications may also implement their own access control systems that restrict use of individual components of the application.
  - For example, an administrative user within the application may see a menu that allows them to add or delete other users.
  - A basic user would see this menu and would not have access to that functionality within the application.

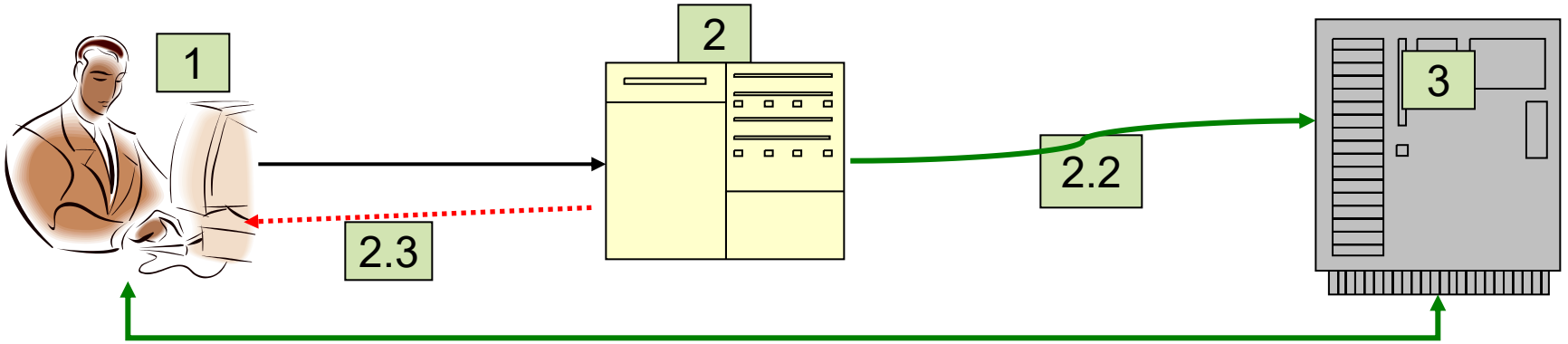
Objects

- System—
  - A system is also a security object. For example, you may restrict access to the CEO's laptop so that only the CEO and his or her administrative assistant have permission to log on to it.
- Operating system—
  - This provides various user modes, such as privileged or superuser mode, user mode, and guest mode.
  - It also governs configuration files and log files.
  - The operating system also provides write protection on files, subdirectory permissions, and restrictions on the ability to create, delete, access, or execute new files or directories.

Objects

- Network—
  - It provides access restrictions for resources stored on the network or on a subnetwork.
  - It provides the ability to traverse network connections and restricts external access, either inbound or outbound.

User IAA Process



1 Identification—User presents credentials:

Account Name & Password (Passphrase, Tokens, and Biometrics)

2 Authentication server Operating System:

1. Receives and compares credentials with authorized credentials
2. If matched correctly, access granted otherwise denial notice sent to user

3 Authorization—Mainframe application server or database:

1. Recognizes authorized credentials
2. Facilitates requests of authorized resources
3. Denies access to unauthorized resources

Secure Management

- Proposed and executed one or more feasible security policy
  - Access-control-policy is high elasticity that authorizes a group of users to perform a set of actions on a set of resources.
  - Some sort of industry guidelines train and teach employee the computer security concept.
  - Incident response plans are the standard procedures for dealing with emergencies

Access Control Systems

A well-defined access control system consists of three elements:

- Policies—Rules developed by someone with a strong knowledge of the organization, its assets, goals, and challenges
- Procedures—Nontechnical methods used to enforce policies
- Tools—Technical methods used to enforce policies

Cyber Security

- Internet now is a new battlefield that everyone in Internet everyday
  - Intrusion prevention system (IPS) monitor, identify and log information network and/or system activities for malicious activity.
    - Attempt to block/stop activity, and report immediately.
  - Social engineer is manipulating people into performing actions or divulging confidential information, rather than by breaking in or using cracking technique.

Levels of Security

- Facility Level
- Network Level
- OS & Application Level
- Data Level Lists

- Physical Controls
- Access Controls
- Video Surveillance
- Background Checks

- Multilayer Firewalls
- Intrusion Detection
- 128 bit TLS Encryption
- Dual Factor Authentication

- Access Control Lists
- User Level Access
- File/Data Integrity

- ADFS & SAML
- Access Control & monitoring (AD)
- Antimalware & Anti Spam
- Patch & Configuration Management
- Secure Engineering

In Cloud Computing

- Properties of cloud computing reduce the part of security issue
  - The property of availability provides the services anytime and reduce the probability of downtime.
  - The property of scalability avoids the starvation of resource and can accommodate a large number of users.
- But cloud computing still need to maintain a high degree of attention on security
- Cloud computing provides services to everyone
  - There are a lot of sensitive information.
  - User do not want any delay or stop service.
  - Cloud vendor want to more and more users to use cloud service.
- But someone also think this is a business.