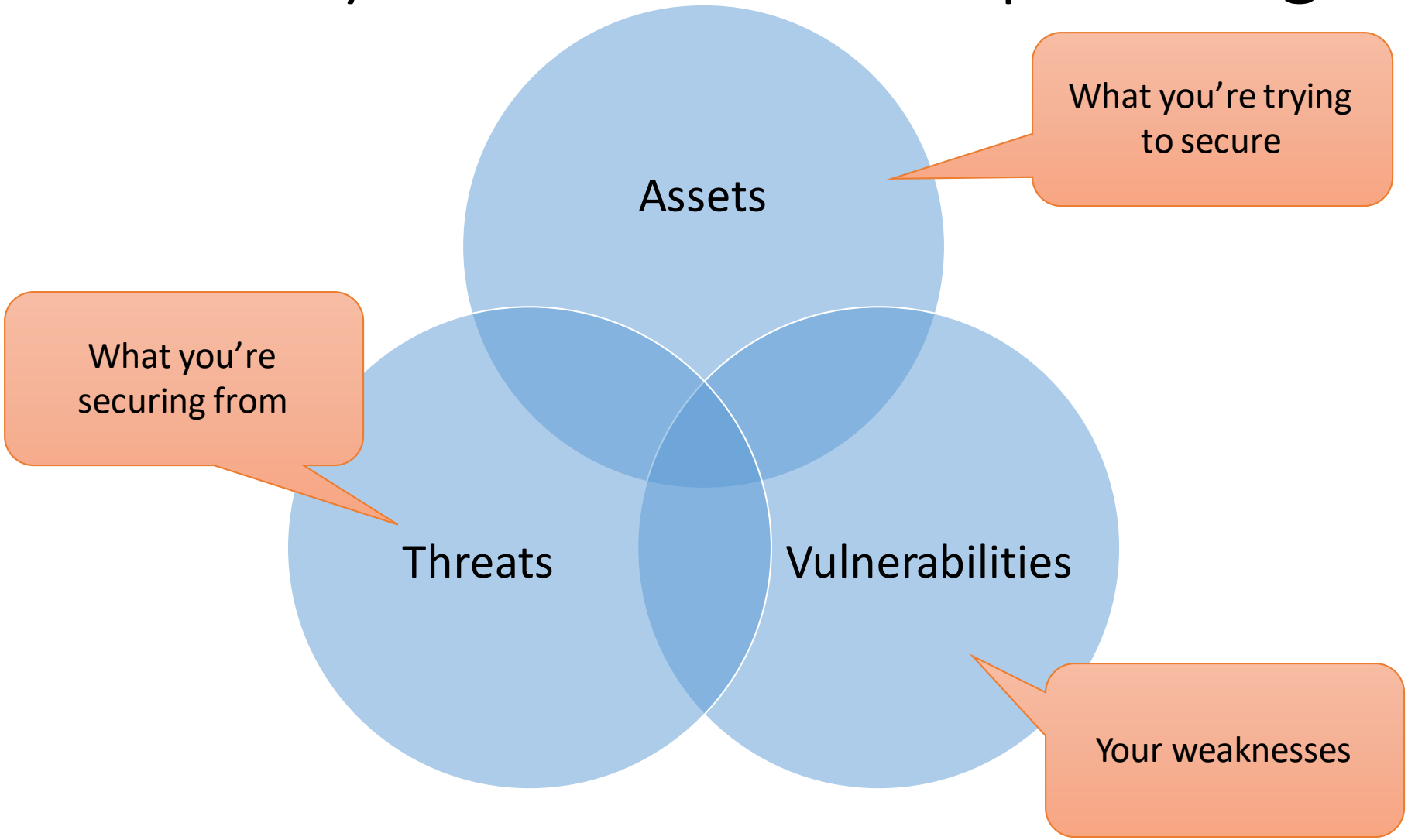
IST346:
Information Security Risk Management

An overview of Information Security

Security is the relationship among



Assets

- The user's **identity** – login, password, personally identifiable information
- Network **bandwidth** – denial of service, bot-nets
- **Storage** / Disk space - warez
- **Data** – the most important asset of them all
- **Reputation** – one incident can ruin a reputation.

Vulnerabilities

- Bad default, or weak passwords passwords.
- Unused services with open ports.
- Un-patched software vulnerabilities.
- Transmitting data in clear text.
- Open networks
- Physical access to systems.
- The users themselves

Vulnerabilities - Social Engineering

- The human element of security
- Users are the weakest link
- Preys on people's inherent trust in others

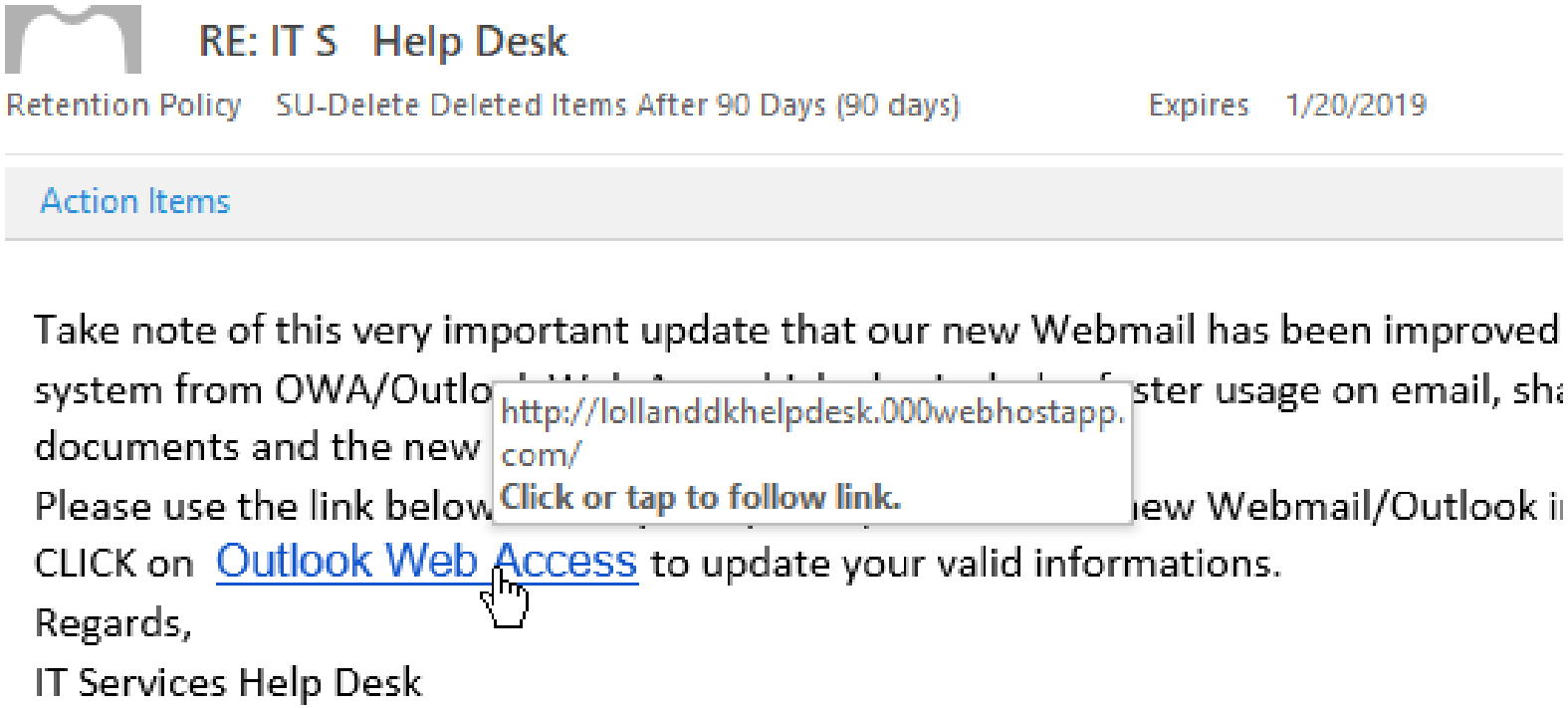
- Kevin Mitnick - Famous Hacker
  - Author of "The Art of Deception" and "No Tech Hacking"
  - One of his many social engineering stories
  - http://www.youtube.com/watch?v=8L76gTaReeg

Threats

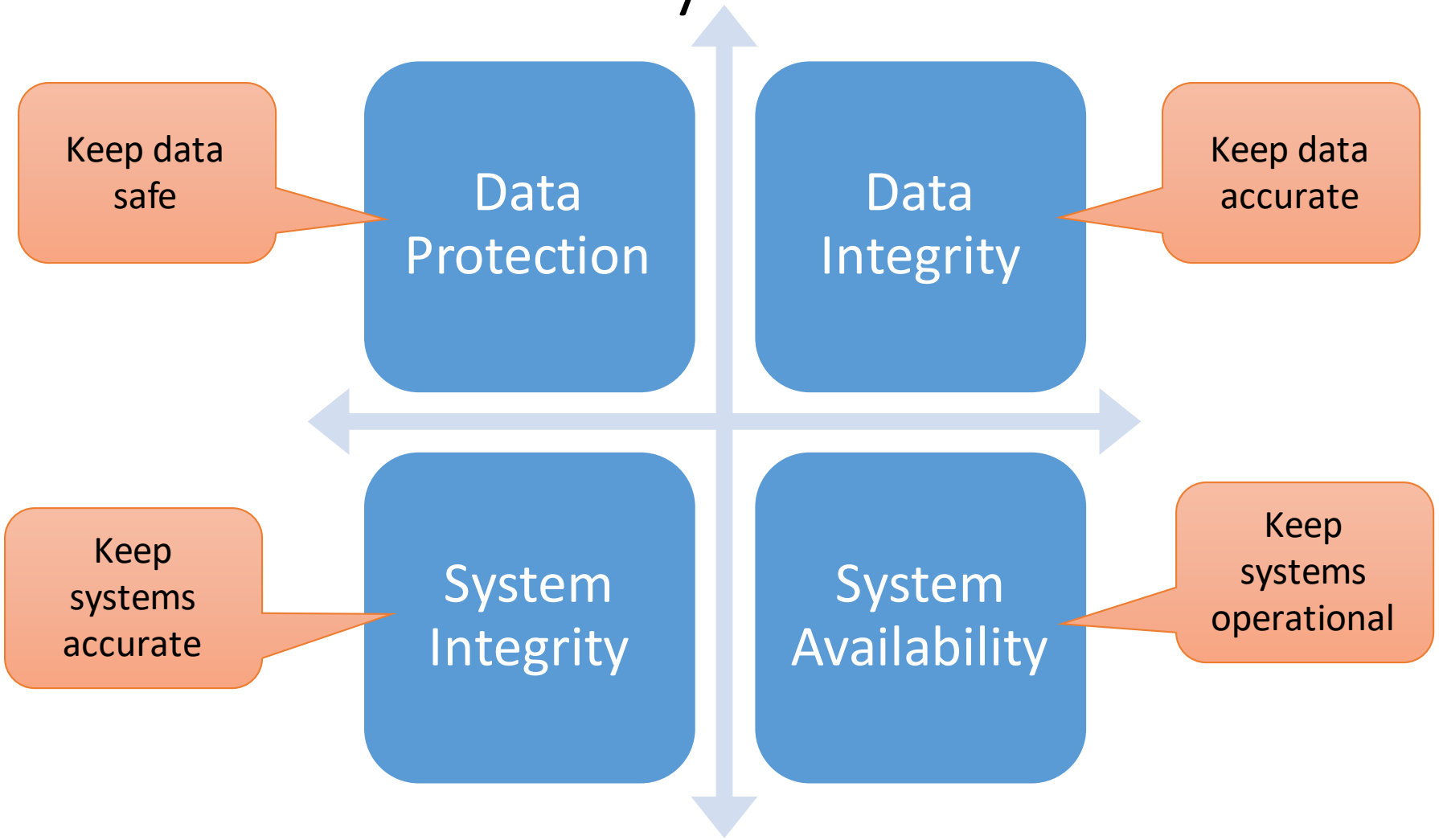
- Financial motives
  - Identity theft
  - Phishing
  - Spam
  - Extortion
  - Botnets
- Political motives
  - Danish sites hacked after Mohammed cartoons.
- Personal motives
  - Just for fun.
  - Insider revenge.

Phishing

- The link in the email doesn't take you where you expect it to go



Goals of Security:



“To protect and to serve your systems and data.”

Can you beat “them”?

- Indefinitely – No. The odds are against you.
  - One in the “herd“ will be lost due to:
    - Software exploit
    - Bad practice
    - Dedicated Hacker
  - All servers shouldn’t be lost.
- Why?
  - You don’t choose all of the applications that run in the env.
  - You don’t write all of the applications that run in the env.
  - We aren’t all security experts
  - Compromise – it happens.

Reducing Risks

What we can do?

Defense in Depth

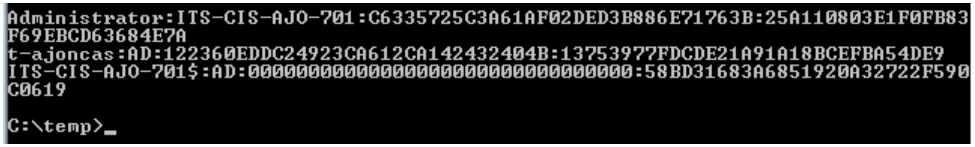
- Secure systems at all levels:
  - OS hardening
  - Application Hardening
  - Network Segmentation
  - Detection of changes
  - Credential Security
  - Encrypting data/traffic
  - Log aggregation (prevents covering of ones tracks)
  - Review Logs regularly
  - Security scanning (open ports, suspicious activity)
  - Security audits (physical, credentials, permissions, pen-tests)

OS / Server Hardening

1. Secure the physical system.
2. Install only necessary software.
3. Keep security patches up to date.
4. Delete or disable unnecessary user accounts.
5. Use secure passwords.
6. Disable remote access except where necessary.
7. Setup least privilege access.
8. Run publicly accessible services in a jail.
9. Configure firewall on each host.
10. Document security configuration.
11. Secure password management.
12. Use secure management endpoints
13. Using a management framework
14. Reduce/Remove elevated credentials

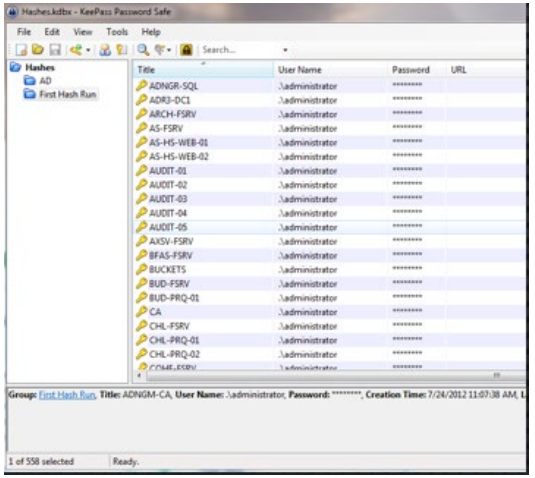
Reducing/Removing Elevated credentials

- Limited User < Local Administrator < System
- Credentials are in Memory
  - Log Off
  - Clear text Passwords
  - Password Hashes
    - 15+ char.



- Service configuration
  - Creating specialized service accounts
  - Limited users preferred, Local Administrators are a compromise
  - Don’t run services as your “admin” account

Credential & Password Management



- 15 + Characters
  - Length > Complexity
- What do you mean password management?
  - There are two common password management Methods…
    - Consistent Passwords Reuse
      - Efficient for you and a Hacker
    - Passwords are written down
      - Where?
      - Is it Encrypted?
      - DR?
  - Alternatives - Unique random passwords
    - USB with Secure Password storage, 2nd factor using Encryption
    - Rubric – “decoder ring”
      - Beware of “homemade” hashing functions

Encryption and Hashing

- Unencrypted data is called plain text ;encrypted data is referred to as cipher text
- **Encryption** is the conversion of data into a form, called a cipher text, that cannot be easily understood by unauthorized persons or systems.
- **Decryption** is the process of converting encrypted data back into its original form, so it can be understood.
- To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
- **Hashing** is a one-way cipher. The text cannot be decrypted. Passwords should be stored as hashes.

Encryption - SSL

- Offers secure transmission between client and server at the lowest level – socket level, sits atop TCP.

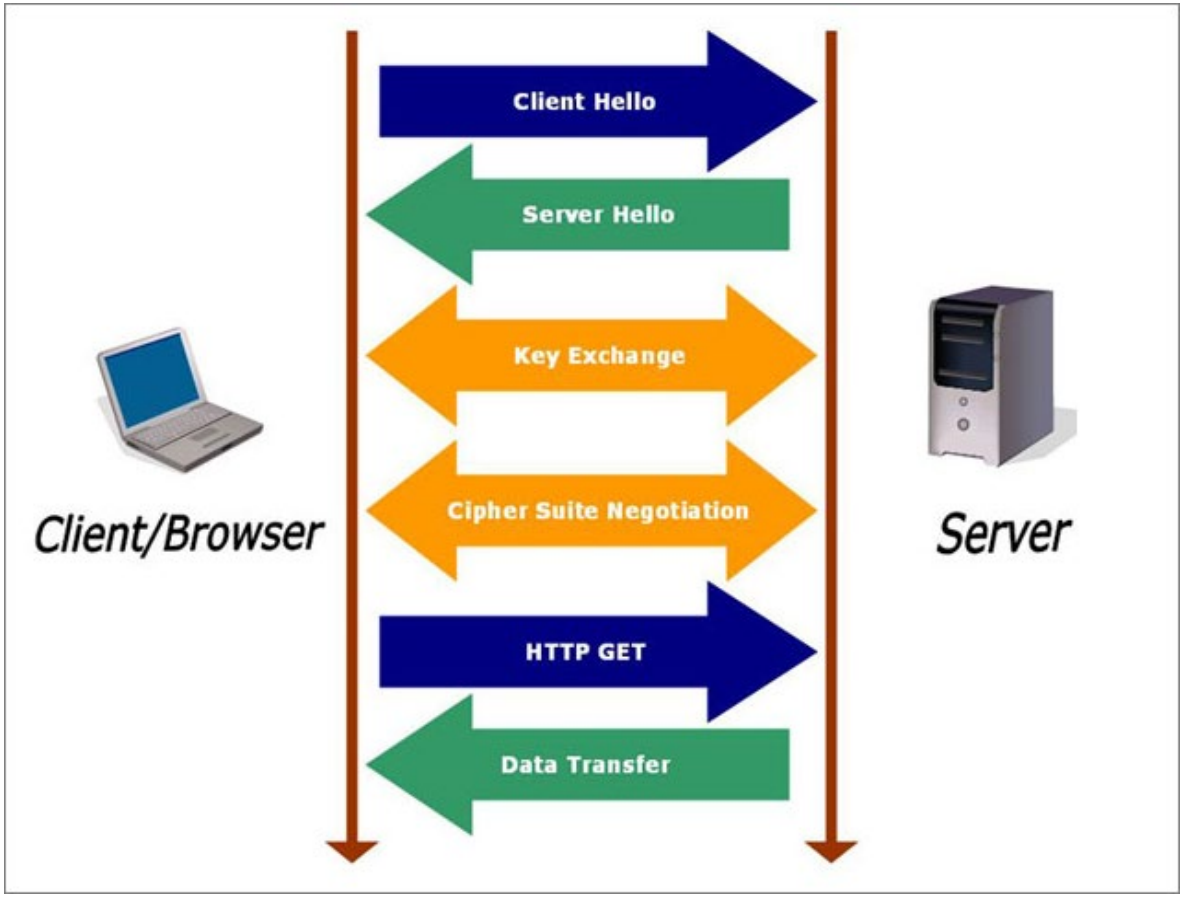
- Two types:
  - Self-signed – certificate created by the host/service you are connecting to.
  - CA issued – an intermediate Certificate Authority issues a certificate that both the server and client "trust"

- Certificate Authorities can be both public and private.
  - *Internet-based services ultimately require a Public CA to assure a proper trust chain be established.
  - Intranet-based services can utilize a Private CA as the trust can be established within the organization.

  - *Clients trust public CAs if they are able to obtain their public key in the browser certificate store.

SSL – how it works on the web

1. Client request
2. Server response
3. Key exchange
4. Cipher negotiate
5. Client http get
6. Data transfer



Defenses

Vulnerability mitigation

- Use secure authentication systems.
- Deploy software in secure configuration.
- Patch security flaws quickly.
- Restrict physical access to systems

Attack mitigation

- Firewalls to prevent network attacks.
- IDS to detect attacks.
- Virus/spyware scanners.
- Disk Encryption
- Two-factor authentication

System Administrator & User Education and Awareness

- Prevent Social engineering
- Prevent Credential Theft

Two-Factor Authentication

Example factors are:

- Something the user knows (password, PIN)
- Something the user has (token, smart card, cell phone)
- Something the user is (biometric characteristic, Physical Location- GPS)
  - RSA Secure ID, Google Authenticator, Duo Security

- Differences?
  - RSA – Type your full password prior to Logon
  - Smart Card – don't type your password, just a PIN
- Still In Memory on the Destination

Considering the pivot Points

- Pivoting
  - They will be inside the Datacenter
  - They will be looking for the next Hop
- When a server is hacked – what else will fall?
  - Does this server NEED to talk to anything else?
  - What's on it?
  - What could it be used for?
  - Do you have any other lines of defense?

Security Policy / Incident Reporting

Security Policies

User Level Policies

Users must sign before receiving resources.

1. Acceptable Use Policy
2. Monitoring and Privacy Policy
3. Remote Access Policy

Business Level Policies

1. Network Connectivity Policy
2. Log Retention Policy

What is an Incident?

Any violation of security policy:

- Unauthorized access of information
- Unauthorized access to machines
- Embezzlement
- Virus or worm attack
- Denial of service attacks
- Email spam or harassment

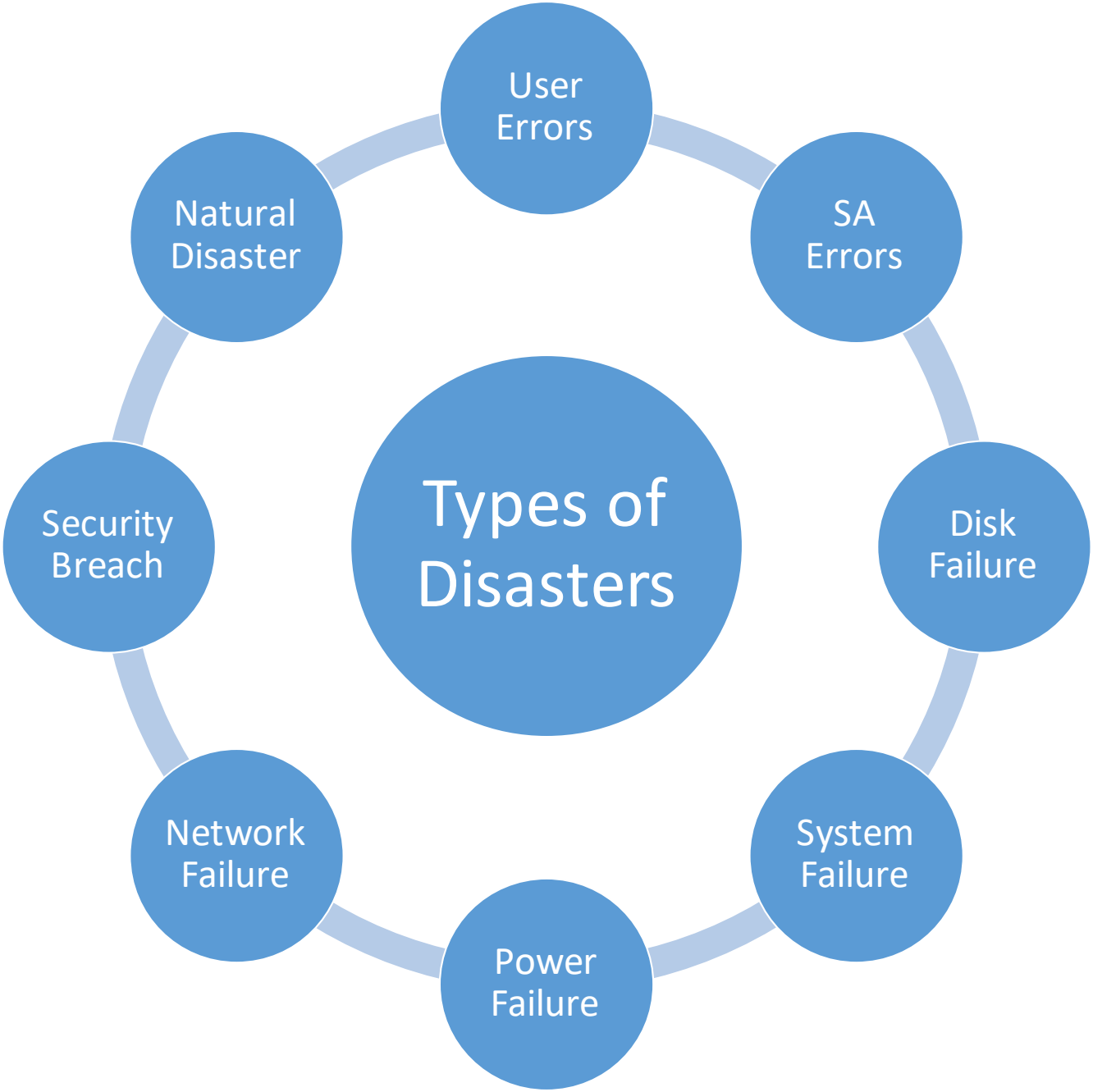
Incident Response Goals

1. Determine if a security breach occurred.
2. Contain intrusion to prevent further damage.
3. Recover systems and data.
4. Prevent future intrusions of same kind.
5. Investigate and/or prosecute intrusion.
6. Prevent public knowledge of incident.

Risk Analysis

Risk Analysis: Some basic terms

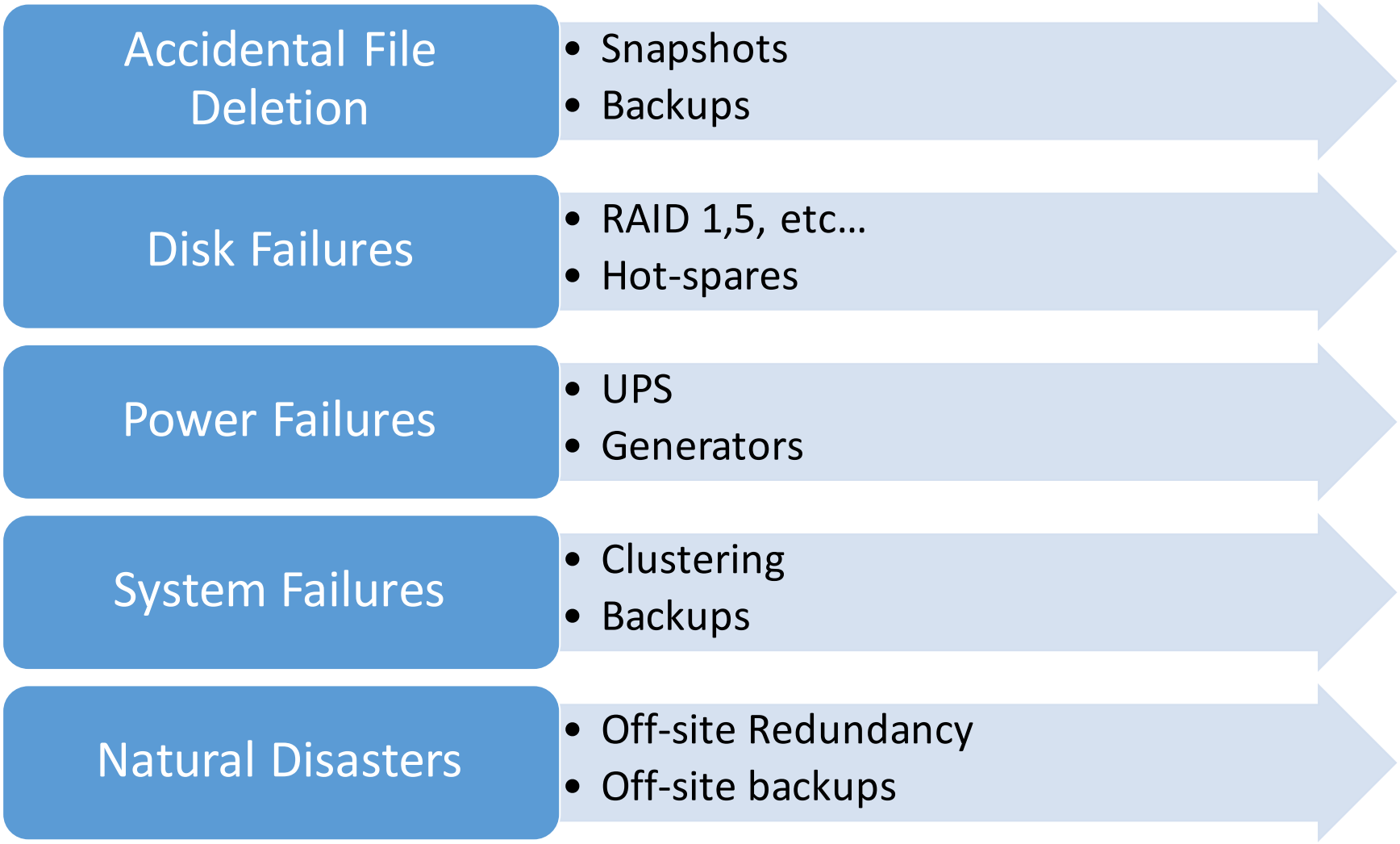
- **Disaster** any event that causes a massive outage to services and/or a loss of data.
- **Severity** of any disaster depends on:
  - How many people are affected (size)
  - Which aspects of the business are affected (cost)
- **Risk** the expected value of the disaster happening in the future.
  - Risk is measured as a probability


Types of Disasters
User Errors
SA Errors
Disk Failure
System Failure
Power Failure
Network Failure
Security Breach
Natural Disaster

Ways we mitigate disasters

- **Fault Tolerance** the property that enables a service to continue operation amidst a failure
- **Redundancy** the duplication of components in a system to increase reliability
- **Backups** copies of point in time data stored separately from the source.
- **Snapshots** point in time copies of data stored on the same source.
- **Service Contracts** lower vendor response times in your service contracts. Store parts on the shelf.

Disaster Mitigation



Example: Calculating risk

- Example:
  - 8 Drive disk array
  - Lifetime 5 years (43,829 hours)
  - MTBF for each drive is 200,000 hours
  - Array Rebuild rate 10 hours.
  - Warranty: 4 hour response, 48 hour replacement of spare parts
- Risk:
  - RAID 0: MTBF = 200,000/8 = 25,000
  - Almost guaranteed chance it will fail over its lifetime 43,829/25,000 (high risk)
  - Of course you would almost certainly use RAID 5 in this case…

Example: Calculating risk

- Risk:
  - RAID 5: System does not fail until you lose 2 disks thanks to one level of redundancy.
  - So where is the risk? Losing another drive in the window between when one fails and the array is rebuilt with the replacement drive.
  - Risk window: your response to the fault + vendor response time + time for replacement part + array rebuild time
  - Risk window: 4 + 4 + 48 + 10 = 66 hours
  - MTBF of remaining array 200,000/6 = 33,333
  - Risk Rate: 66/33,333 = 0.2% or 1 in 500.

Example: Calculating risk

- Risk Rate:
  - Is a 0.2% chance of failure an acceptable amount of risk?
  - How can we lower the amount of risk in this case?
  - If we can lower the risk by a factor of 10 to 0.02% for a cost of $25,000 is it worth it?
  - What does the acceptability of this risk (or any risk) depend upon?
  - For example, are these two risks the same?
  - 0.2% chance of failing a course vs. A 0.2% chance of dropping out of school.

Budgeting for Risk Mitigation

- Risk Budget = Risk Rate * (Estimated cost of disaster – Estimated cost of mitigation)
- Example (from before) when that storage array becomes unavailable it will cost the company $10,000/day and be down for 10 business days.
- Risk budget = 0.002 * ($100,000 – $0) = $2,000
- That $2,000 could be spent on hot-spare and perhaps a RAID6 configuration.

Budgeting for Risk

- Single Events
  - Cost should datacenter be destroyed: $60 million
  - Risk of Flood one in 1 million
  - Risk of Earthquake one in 3000
- Flood Risk budget = (0.000001)*$60,000,000 = $60
- Earthquake Risk budget = (0.000333)*$60,000,000 = $20,000
- So, you should budget and plan for an earthquake but not a flood. Why?

Budgeting for risk

- A small on-line retailer cannot make $$$ when their internet connection is down.
  - It goes down, on average for 2.5 hours each month (every 30 days), in periodic intervals. As per the ISP's Terms of Service.
  - The company estimates they lose an average of $15,000 for each hour their connection is down.
  - What is the Rate of failure for this internet connection?
    - 2.5 hours / 30*24 hours = 0.0035 This is the risk rate each month
  - What is the loss of business each month?
    - 2.5 * $15,000 = $37,500 /month
  - What should the monthly Risk budget be?
    - 0.0035 * ($37,500 - $0) = $131.50
    - It makes sense to get a secondary internet connection if you can find one for less than $131.50/month.

Disaster Recovery and Business Continuity

Disaster Recovery Plan

- *Defined*: The process that allows a company to recover all systems, data, services, etc. May take hours, days, or weeks depending on number of systems used and their complexity.
- Help prevent a IT Disaster From Happening in the 1st place:
  - Implement fault tolerance components and a solid backup and recovery strategy
    - Types of Fault Tolerance components:
      - RAID'ed hard drives
      - Redundant paths to your IPS or redundant IPS'
      - Backup power via UPS or generator (or both)
      - Mirrored copies of data located off-site
      - Mirrored servers (clusters)
      - VMWare or imaged servers
  - Read manuals and pay attention to what you are doing.
  - Isolate systems from other systems or to restate, don't run multiple services on the same server.

What is a Disaster Recovery Plan?

A DR Plan…

- Considers potential disasters.
- Describes how to mitigate potential disasters.
- Makes preparations to enable quick restoration of services.
- Identifies key services and how quickly they need to be restored and in what order.

Only High-Risk / High cost plans should be considered

Disaster Recovery Plans

1. Define (un)acceptable loss.

   Data? Productivity? Re-Creatable data? At what cost?

2. Back up everything.

   Backup data, metadata (config), and instructions on how to restore your system.

3. Organize everything.

   Can you find the backup tapes you need when disaster strikes? Make sure everything is clearly labeled.

Disaster Recovery Plans

4. Protect against disasters.

   Natural disasters with high probability and many more.

5. Document what you have done.

   Plan must be detailed enough for people to follow in a disaster w/o additional info. Hardcopies are key.

6. Test, test, test.

   A disaster recovery plan that has not been tested is not a plan; it's a proposal.

Disaster Recovery Plan Ideas

- Many places have a DR plan that says something like “buy new hardware, re-install our OS, applications, then restore our databases or data files from the previous backups”
- What’s wrong with this plan ?
- How long do you think this will take, a week, 2 weeks, a month?
- What ‘data’ do you need to include? Is it up-to-date at your “DR” location?
- To protect against or minimize data loss, data can be ‘copied’ either periodically (asynchronous) or in real-time (synchronous) from one server to another for DR processes.
- Ideally the servers should be in different buildings, campuses, or even states as to guard against large scale natural disasters.

Asynchronous Replication

- **Defined:** Data is refreshed or synchronizes periodically (most commonly done once per day) during periods of inactivity (night).
- Advantages of asynchronous replication
  - Typically is less expensive. Don't need to invest in sometimes expensive data replication software. Can use free tools, ex: Robocopy.
  - Can be used to restore data from.
  - If your data files are only refreshed nightly, the target location can be used to restore data from in the event a user deletes or corrupts data during the day or a user deletes a file.
- Disadvantages:
  - Data is not kept 100% up-to-date at secondary site. If you run a bank or hospital, this may cause health, legal, or financial issues !

Synchronous Replication

- **Defined:** Data is replicated from primary site to secondary site in “real-time - automatically”. No period sync process
- Advantages of synchronous replication
  - Data is always up-to-date at secondary site. Don’t need to worry about what ‘work’ needs to be re-entered by your users.
  - If you are replicating from SAN to SAN, you may be able to use some of the DR hardware at secondary site for non-production purposes (allows your servers to do double-duty) such as to run reports. If needed, this DR hardware can quickly be re-setup for production need. Works great if you are using virtualization.
- Disadvantage:
  - Costs money, may requires additional products (cost), and adds complexity to running systems

Business Continuity

- The organization's ability to continue to function during and after the disaster.
  - Think of BC as your fallback plan for the disaster.
- It is not the same as disaster recovery, but ultimately a part of it.
- Example:
  - Labor Day storm 1998. Power was out for 10 days.
  - The company I worked for had a BC plan. They'd better they were in the business of selling generators!
  - Sales and Rentals would be processed manually (on paper) and then recorded into the system when it came back on-line.

Business Continuity, another example

- Snowstorm in 1997. Computers across an entire organization's site were down when snow took out their terrestrial satellite links (wide area network for them at the time.
- The company I worked for had about 2000 employees and manufactured medical diagnostic equipment, so had to perform support for doctors offices, hospitals, and surgeons daily.
- The customer service departments kept printed and bound copies of all of the service manuals for every piece of equipment the company had ever designed at their desks. When the network was down they could not access the electronic manuals, so the were able to fallback to the printed copies.