Cybersecurity Investigations and laws

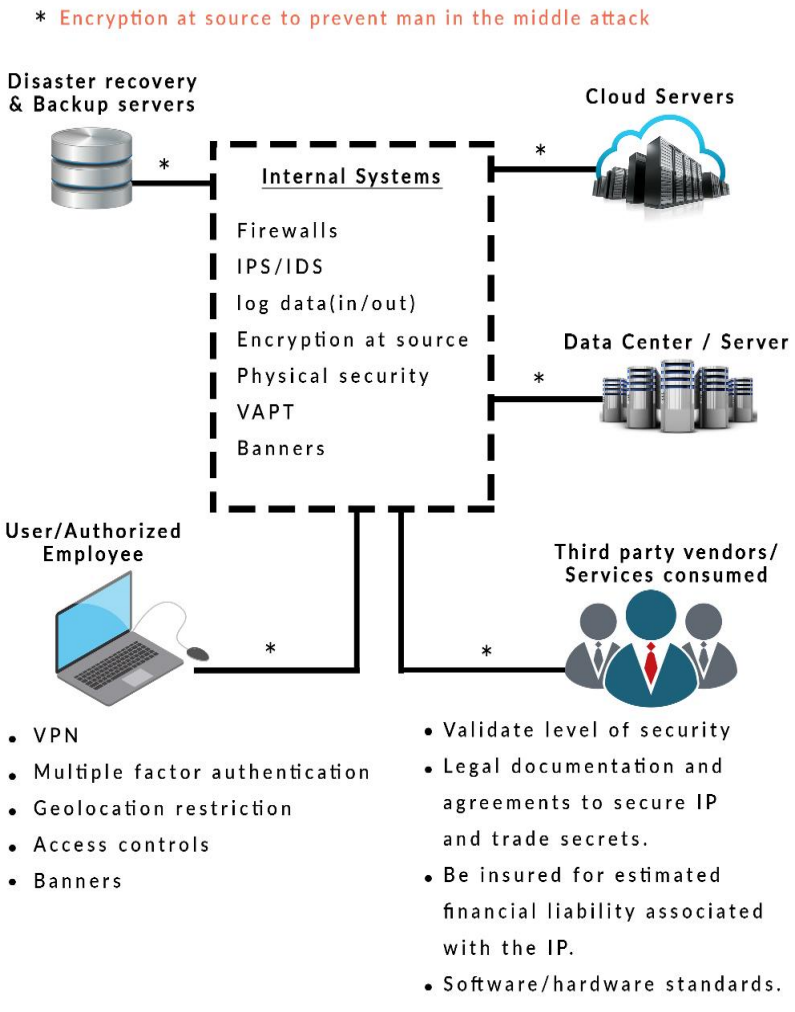
CS 698

Assignment 2

Hawk eyes: **Adhithya Sivanesh (as3423), Gautam Pandey (gp88), Ketaki kakade (kk524)**

Vendor management comprises of all of the processes required to manage third-party vendors that deliver services and products to companies. Significant effort is required from both the institution and the third-party vendor to maximize the benefits received from the relationship, service, or product, while simultaneously minimizing associated risks. The increased use of outsourcing to third-party vendors and the importance of the relationships between the company and those vendors intensify the need for the companies to have highly effective third-party vendor risk management programs in place.

Following is the basic layout of the internal network of a company and the associated vendors and communications between them.



A company has the following components that are associated with the third party vendor:

1. Cloud Servers
2. Data Centers / Data Servers
3. Products or services consumed using third party.
4. Disaster recovery and Backups

Risks of using third party vendors

When a company uses a third party vendor for its services, might it be for cloud or data servers, third party products that are used by the company, are susceptible to the vulnerabilities and breaches and other risk factors.

1. Unauthorized access to customer and business data

When a company outsources its information technology, it is placing its trust in a third-party – relying on their expertise, their resources, and their services. Ideally, the transition works out. Once a company outsource a service to a third-party server, the company now have to worry about its staff and the vendor's staff. More people have access to the data and systems that support the service which might be an access point for an attacker to enter into the company's internal network.

2. Security risks at the vendors

While using a third party for its services or outsourcing its information technology a company barely checks things like

1. The character of the vendor's employees
2. The security of the vendor's technology
3. The access the vendor has to their data

The company's reputation no longer depends on the integrity of only its business – now it also depends on the integrity of the vendor's business.

3. Compliance and legal risks

Many data security regulations are intended to protect a specific type of data. For example, HIPAA requires healthcare providers to protect patient data. PCI DSS requires anyone who accepts credit cards to protect cardholder data.

Not only are the companies covered by these regulations required to protect the data, they are also typically required to know

1. Where the data resides
2. Who is allowed to access it
3. How it is protected

If a company outsources the processing or storage of data that it is required to protect, then it is relying on a cloud service provider to maintain their compliance. If the company does not have

adequate legal protections, then it may be liable when there is a data breach at the cloud service that exposes the company's data.

4. Risks related to lack of control

When a client host and maintain a service on a local network, then the client have complete control over the features you choose to use. If he wants to change the service in the future, he has the control. However, when a client uses third party services, the vendor is in control. He has no guarantee that the features he uses today will be provided for the same price tomorrow. The vendor can double its price, and if client's customers are depending on that service, then he might be forced to pay.

The following are the associated risks for outsourcing certain components to third party:

Cloud Server

1. Cloud services aggregate data from thousands of small businesses. The small businesses believe they are pushing security risks to a larger organization more capable of protecting their data. However, each business that uses a cloud service increases the value of that service as a potential target. This concentrates risk on a single point of failure. A disaster at a cloud provider can affect every one of its customers.
2. When a cloud service vendor supplies a critical service for a company and stores critical data – such as customer payment data and the mailing lists – the life of the business is placed in the vendor's hands.
3. A breach of any data or the client's data can be devastating depending on the type of data and the extent of the breach.

Data Center / Data Servers

1. They are prone to physical security issues like natural calamities, issues due to maintenance failure, sabotage and could also be prone to virtual security issues like virus, spam, hacking, stealing of data etc.
2. The reliability is a major issue. For example, there could be a server downtime, network connectivity problems or related issues.
3. The intellectual property could be at risk. For example, Competitors could bid to hack into confidential data.
4. Often companies feel that having a data center enhances the reputation. This is true only to the extent that it is owned by itself, and is not outsourced to any third party vendor.

Products or services consumed using third parties:

1. Failure to properly assess, understand, and document the risk and cost of outsourcing services.
2. Failure to perform proper due diligence and ongoing monitoring.

3. Entering into contracts without a proper assessment of the third-party's risk controls.
4. Entering into contracts that could incentivize a third party to take risks in order to maximize profit, even if those risks could be detrimental to the organization.
5. Engaging in third-party relationships without a formal contract, or with inadequate contracts.