ISEC0655 FALL 2022 ASSIGNMENT #1 JASHOPPER EXECUTIVE SUMMARY

By Eric Webb

What business and industry is Secom operating in?

- Started with physical security which evolved into digital surveillance.
- Joint ventures in TV and Telecom.
- Began hosting services such as Web hosting, CA’s, and data warehousing.
- Made GPS trackers.
- Information security services such as Firewalls, IDS, and IPS.
- Security consulting services.

What are its strengths and weaknesses?

	Helpful	Harmful
internal Origin	Strengths - Experience - Ability to Adapt - Innovators - Hard work ethic	Weaknesses - A main single SDC - Big Target
External Origin	Opportunities - Background and resources to innovate.	Threats -Insiders Threats - External Threats -Politics -Unseen trends in technology

Who are their customers and what do they do to satisfy them?

- Companies that need physical security
  - Guards and surveillance systems.

- Companies that need cybersecurity and IT services.
  - Hosting, SSL certificates, network infrastructure, & data warehousing.
  - IDS / IPS / Firewalls.
  - Security Audits.

What is the main problem and decision to be made in the case?

- Main problem is that Jashopper needs to increase their security posture but does not have unlimited funds and resources to do so.

- The decision to be made is choosing the best plan to fit Jashoppers risk appetite.

What facts are relevant to a solution?

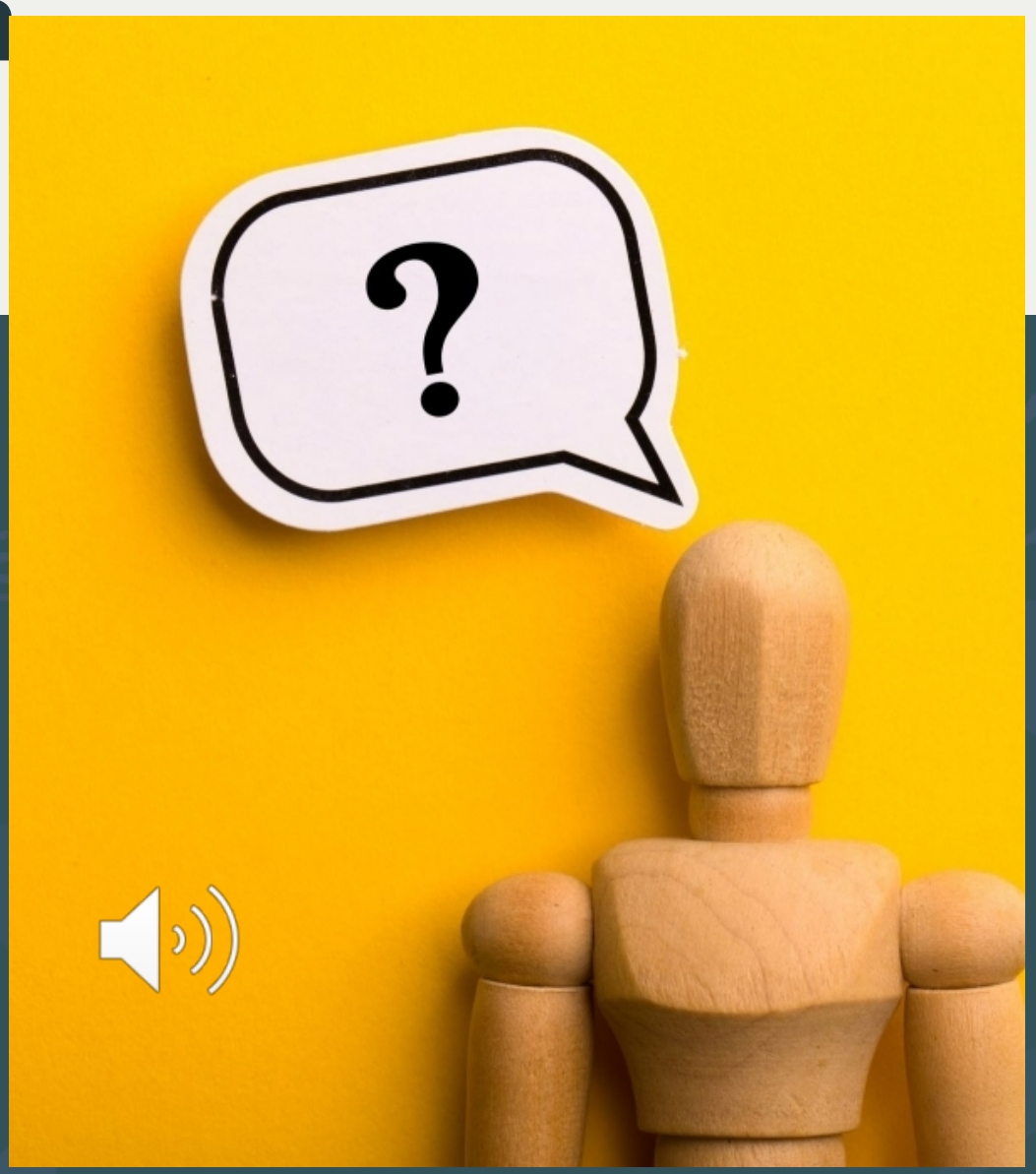
- Most information leaks incidents are from insiders.
- There is no guarantee of security.
- Internet population and penetration is growing.

What are the decision criteria?

Current business needs.
- 5 Servers
- 6 IP addresses

Future business needs.
- Ability to scale
- Ability to manage

Risk appetite.
- Budget vs risk tolerance

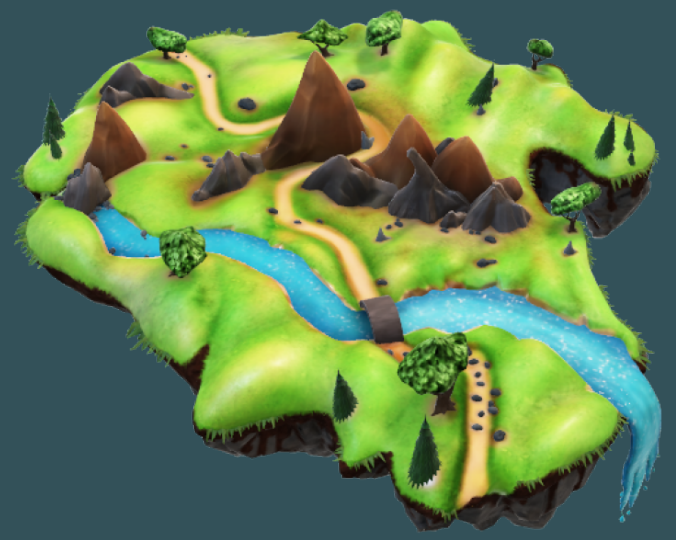


What are the risks?

- Could outsource IT security infrastructure and still be breached.
  - Risk of Secom getting hacked and Jashoppers data being compromised.
  - Risk of faulty configurations and dependent on Secom for emergencies.
- Could build IT security infrastructure in house and still get breached.
  - Vulnerable to the natural growing pains of building in house.

What are the alternatives?

- Outsource for short term gains.
- In House for long term gains.
- Mixture of both.



Provide your evaluation of each alternative given the decision criteria.

	Outsource	In House	Mixture of Both
Pros	Don't have to build your own infrastructure. - May be cheaper to outsource with better coverage. You Inherit knowledge from their previous trials and errors. -Secom has put in the time and effort over the years to gain this knowledge and position which will reflect into Jashoppers IT security posture.	Not dependent on 3rd parties. - 3rd parties can stop services at any time for what ever reason or get breached. More control over IT infrastructure. - Can do what ever you want to with your infrastructure and not be limited to that services products.	Get flexibility over IT infrastructure. - Can control in house network while still providing services to customers through outsourcing. Still having piece of mind. - 3rd parties take on some risk bearing some risk load off Jashopper.
Cons	Dependent on outsourced provider. - Can be breached from insiders or outsiders still. - Can be a lack of services offered and options for configuration. - Can be a lack of communication between parties involved. - -Dependent on 3rd party incase of emergency.	Dependent on inherit knowledge and resources. -More prone to mistakes when growing in house. -Less experience and guidance. -Costly.	Some things might not interface well or leave pockets of vulnerabilities. - Where IT infrastructure meets between parties might not interface well. - Pockets of vulnerabilities can manifested where overlooked.

Provide your recommendations to the board and justification

- My recommendation is to go with a mixed approach.
  - The 3rd party does offer services that can be beneficial to outsource.
    - I would recommend E-Document solution to handle Japan's E-Document law.
    - I would recommend the Digital Certificate Service for encrypting transactions and securing site.
    - I would recommend the normal Server Hosting.
    - I would recommend Firewall Services.
    - I would recommend audits.

  - A lot of these products are overkill for the business needs.
    - Don’t need IDS/IPS.
    - Don’t need Identity and Access Control Systems.

Describe how you would implement your solution.

- Step 1 : Copy Consumer Information to E-Document service.
  - I would recommend doing this first because it satisfies the law and should be less painless than the next the steps.
  - It will also establish business relations to see if you want to carry on with the next deals.
- Step 2 : Set up new hosted servers with test website environment.
  - I would recommend setting up the current production code on the newly outsourced server but keep them local and private from the outside world. The original production code is still being used until it is time to integrate.
- Step 3 : Set up SSL Certs from CA Service to test environments to verify security.
  - I would recommend setting up the SSL Certificates through the Certificate Authority Service.
  - Verify local outsourced environment is working with automated testing and that the SSL is applied.
  - Verify shop owners can login to their interface.
- Step 4 : Expose website to outside world through firewall service set up load balancing.
  - Only allow ports needed, explicit deny all the rest.
  - Set up load balancer functionality to route all traffic to new web service.
- Step 5 : Run audit on network.
  - Run 3rd party audits on new outsource network preferably from someone other then Secom's own audit on itself.
- Step 6 : Make the switch to production over time.
  - Set productions IP address to new load balancer address and have 10% of traffic go to new services and 90% to old services.
  - If things go smooth gradually adjust those metrics over time to ween off the old services.
  - Can keep a small amount of traffic inhouse for redundancy for emergencies. (5% traffic)

Predict and justify the results

- I believe this solution will go over well because it has a fault tolerant solution through the load balancing.
- If things go bad the load balancing can quickly route traffic back to the original services.
- If things go well the new services will be better for the company and give them the ability to scale.

Outline the strategic role of the following organization stakeholders at Secom in planning and governing security

- Board of Directors – They are the supervisory role of the company, they are the ones who the C-level executives report too, They control the flow of money.
- CIO – They engage in IT initiatives and goals they focus on growth.
- CISO – They focus on IT security and protect the company from over stretching its business goals.
- Senior Management – They are the liaisons between The C-levels and the functional area managers. Verifying compliance is met and metrics are achieved.
- Functional area management - They manage the day-to-day personnel and pass ideas from the bottom up while policing from the top down.
- Information security personnel – They are the ones running the show, programmers, network admins, marketers, etc.
- End users – People buying stuff of the website and shop owners.

Research matrix relevant to the utilization of a third-party services

- In my own words matrices usually are just tables of information like excel spread sheets but can arguably any 2-dimensional area of data.
- I chose this Matrix because although it does not provide concrete data points it provides important thought processes when it comes to third parties.

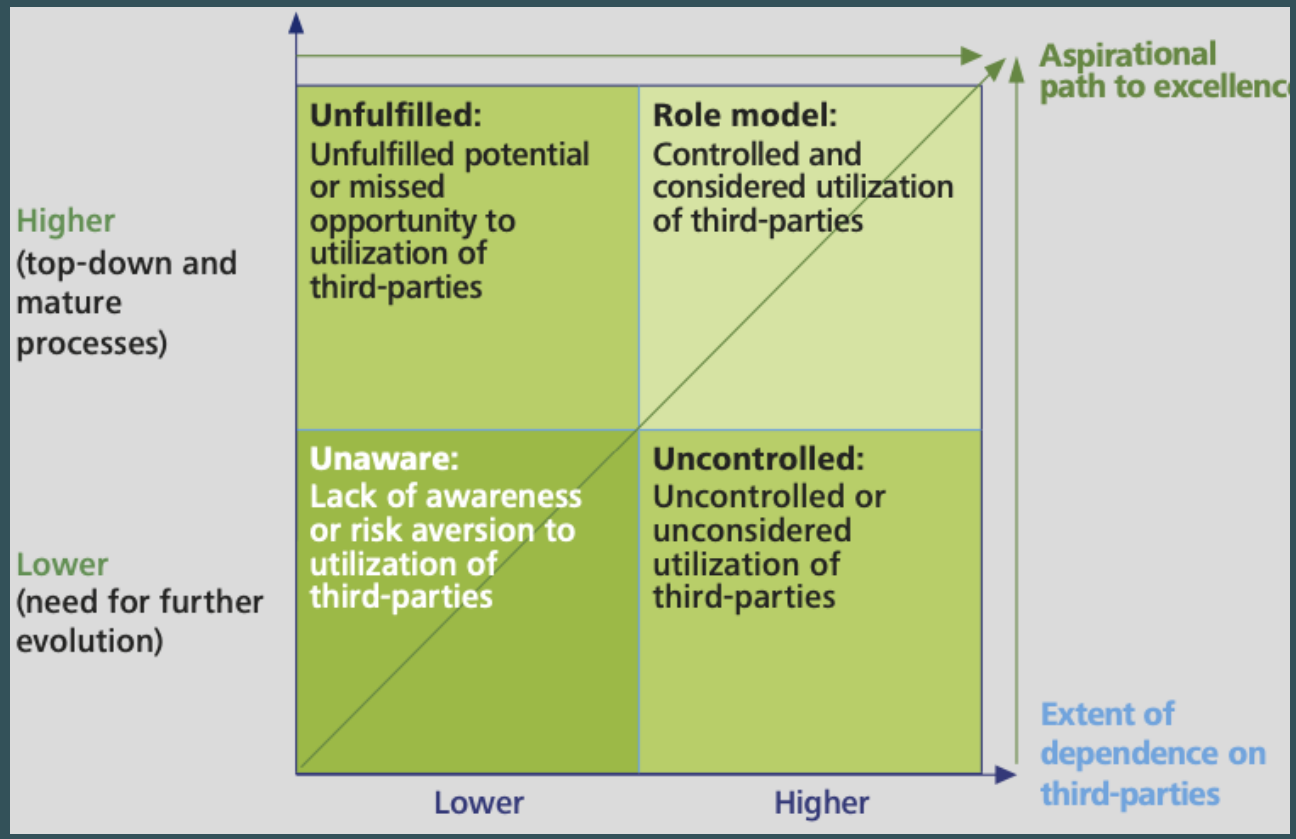
Objective 1: Fulfil untapped potential using 3rd party services.

Objective 2: Avert as much risk as possible away from company via 3rd party services.

Objective 3: Be as independent as possible while still outsourcing.

Objective 4: Be able to grow and scale.

Objective 5: Don't lose security for elasticity.



https://www2.deloitte.com/cbc/en/pages/risk/articles/third-party-governance-and-risk-management.html