ISEC-655 Fall 2022

Dr. Michelle Ramim

Eric Webb

Assignment #1 Executive Summary

November 13th, 2022

Dear Executives,

I have been tasked with conducting a formal review of the services offered by Secom regarding the security posture and scalability of Jashopper. Please see my detailed narrative below for basing future decisions on this subject matter of scaling Jashopper securely.

Thank you again.

- Eric Webb

  (CISSP)

Overview of Secom

Since its conception in 1962, Secom has worked hard to establish its foot hold in Japan's security market. Starting with traditional physical security they have evolved into providing a myriad of physical and digital security services. Traditionally, most companies in Japan provided security inhouse and the concept of outsourcing security was still new. As the digital revolution materialized, Secom began to develop digital security services through CCTV and Digital Sensors. They then again captivated their audience by being able to dispatch staff to check on the situation, which most other companies did not do at that time. As the times grew Secom also ventured into many other projects such as GPS location devices, television, and telecommunications. As this breadth of knowledge solidified, Secom began to find its niche in security services. Not only do they offer physical security services such as metal detectors, retinal scanners, and key cards, but they also developed a whole suite of information security services as a third-party risk management framework. According to a study on third-party risk management frameworks "TPRM frameworks, much like cybersecurity frameworks, are necessary to have an organized approach to reduce risk". (Rasner,2018) One example in this technology suite is tiered server hosting in remote data centers. They offer monitoring and

protection through firewall, intrusion detection, and intrusion prevention systems. On top of all that, Secom is also one of the leading certificate authorities in Japan providing SSL server certifications and client certifications services. To keep companies in Japan compliant with how user data is stored, Secom offers a service for electronic documentation storage. Secom also offers auditing services to revise and propose security solutions.

Description of Issue

Currently Jashopper has a user baser of over 600,000 users, 400 established shops on its website, and 20 employees. The problem is that Jashopper needs to increase their security posture and scalability, but do not have unlimited funds and resources to do so. Because Jashoppers user base is over 5000 they need to be compliant with Japan's Personal Information Protection Law. On top of securing the user data Jashopper plans on scaling in the future and wants to prepare for upcoming growth. It is no secret that information technology is a growing field and having a presence in the e-commerce space is becoming more competitive, Jashopper needs to be able to keep up with this space and remain secure as more users join. As the market matures more opportunity of attack can develop with new vulnerabilities being found and exploited. It is up to Jashopper to handle most of that protection in house or to mitigate some of that risk through a 3rd party. A decision must be made to choose the best plan to fit Jashoppers business needs vs its risk appetite.

Description of alternatives

In this situation there are really a few options. The company can maintain infrastructure in house and establish security locally but sustain all the risk. The company could outsource infrastructure and security taking some risk off Jashopper and on to Secom or any other 3rd party hosting and security provider they deem fit. Lastly the company could go with a multi-layered

approach. This is where some of the services are retained in house while others are implemented through outsourcing. This creates a multi-layered infrastructure that properly mitigates risk where applicable while simultaneously extending the company's business capabilities and needs.

Implementation Plan

In this situation I would go a for a multi-layered approach and gradually ween off the older in-house services to the new outsourced services while still holding on to some capabilities for emergencies.

- 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 should still be used until it is time to migrate traffic.
- Step 3: Set up SSL Certs from CA Service to test environments and verify security.
    - I would recommend setting up the SSL Certificates through the Certificate Authority Service.

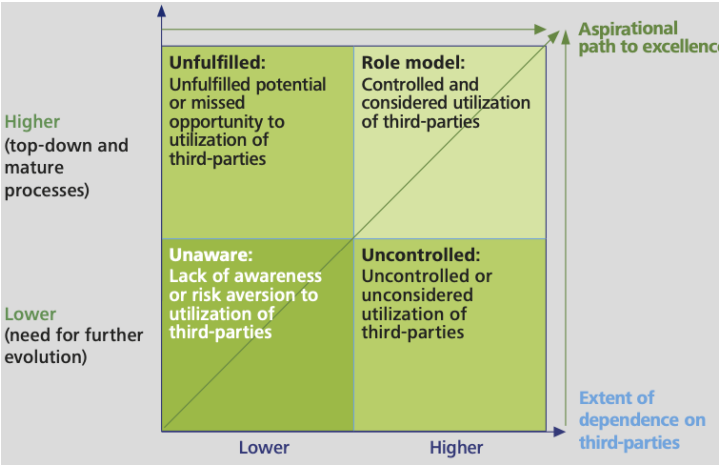
    - Verify local outsourced environment are working with automated testing and that the SSL is applied.
    - Verify that your store owners can now login into the website with their client certificate.
- Step 4: Expose website to outside world through firewall service and set up load balancing.
    - Only 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 outsourced network preferably from someone other than Secom.
    - Also get an audit by Secom to compare findings look for discrepancies.
- Step 6: Make the switch to production over time.
    - Set productions routing to new load balancing firewall service 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.
    - Keep a small amount of traffic inhouse for extreme emergencies or keep unplugged as a cold store that could become operational again in a short amount of time. Don't keep all eggs in one basket.

Planning Roles

- 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 and stakeholders' best interests.
- CIO – They engage in IT initiatives and goals they focus on the growth through IT operations.
- CISO – They focus on IT security and protect the company from over stretching its business goals.
- Senior Management – They will be 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 products from the website and shops who have stores on Jashopper.

Research Matrix

In my own words matrices usually are just tables of information like excel spread sheets but can arguably be any 2-dimensional area of data. I chose this Matrix provided from a Deloitte employee (Ryan, 2016) 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 and giving up control.

Objective 4: Be able to grow and scale.

Objective 5: Don't give up security for elasticity.

Research Matrix

So, in conclusion, through outsourcing IT infrastructure to Secom, I believe the company can put itself in a good position to scale and mitigate some risk. This is through offsite server hosting with certificates supporting security and a firewall load balancing traffic over time from the old infrastructure to the new. Along with other minor beneficiary services that are just simpler to host offsite such as the e-document service or getting an audit. The beauty of going through this approach is that it positions Jashopper to scale and piggyback security from Secom, who is more aggressive in this space. The tradeoff is that Secom is such a larger player in the space that they are more pursued as targets then the lower hanging fruit of Jashoppers in house system. All in all, I would recommend

Jashopper outsource to some services of Secom or other 3rd parties to remain compliant and elastic.

References

Rasner, G. (2018) "Front Matter," in Cybersecurity and Third-Party Risk: Third Party Threat Hunting, Wiley, 2021.

Ryan, O. (2016, June 8). *Third-party governance and Risk Management: Deloitte: Risk Services*. Deloitte. Retrieved November 11, 2022, from https://www2.deloitte.com/cbc/en/pages/risk/articles/third-party-governance-and-risk-management.html

Certification of Authorship of Doctoral Course Assignment

College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

Submitted to: Dr. Ramim

Student's Name: Eric Webb

Date of Submission: November 13th, 2022

Purpose and Title of Submission: Assignment #1 Executive Review

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this purpose.

Student's Signature: ERIC WEBB