IT4983/W01 – Group 7  
Eric Whang, Mark Schuler, Daniel Newman, Alex McMath, Ryan Smith, and Samuel Olubummo

Security Solution for a Small Business: Risk Assessment

First, we have to make some assumptions about our small business. In 2019 the average small retailer with 50 or fewer saw average monthly revenues of $22,341 (Guta). Our hypothetical business distributes PCs, PC components and peripherals which tend to skew expensive, so for our purposes we’ll assume our business is exceptional and we generate revenues of $80,000 monthly or $960,000 annually. Second, our hosting partner (KSU) exercises every conceivable control to restrict unauthorized physical access to our servers and have best in class disaster recovery plans in place in the case of natural disasters. Third, we’ll operate under the assumption our ISP has agreed to a service level agreement of 99% (allowing for roughly no more than 15 minutes of downtime daily) where we’ll be compensated $110 per hour (based on annual revenue) of downtime beyond SLA agreements, to cover lost sales. Finally, though our business ultimately sells physical goods securing inventory, warehouse space, shipping and supply chain stability considerations are beyond the scope of this risk analysis where we will focus on our IT assets.

**Asset Identification**

Our organization’s primary assets are: e-commerce site, server, customer information, customer payment information, supplier information, software configuration information.

**Threat Identification**

Thanks to the tireless efforts of our business partners at KSU whose best-in-class disaster recovery protocols and security measures effectively reduce the threat of hardware failure due to natural disaster or disrepair to vanishingly small numbers that approach zero. Our principal concern will be securing our site against malicious behavior like denial-of-service attacks, theft of data or social engineering attacks.

**Vulnerabilities**

Our main concern is going to be software vulnerabilities: misconfiguration, compatibility issues, possible gaps in our layered defense. The human element must also be considered, accidental file deletion or misuse of admin privileges etc.

**Controls**

We will implement a combination of technical and administrative controls in order to mitigate risk. A firewall will be deployed to filter unwanted traffic and stored data will be encrypted. Administrative controls will include a policy of least privilege for users along with security awareness training.

**Risk Assessment visualization**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Threat** | **Vulnerability** | **Asset** | **Impact** | **Likelihood** | **Risk** | **Recommended Controls** |
| Natural Disasters Medium | Server stored offsite at secure facility Low | Server Critical | E-Commerce site down, lost sales. Critical | Tornadoes, floods are unlikely Low | Low | No action needed at this time |
| Malicious Activity High | Improper Configurations Medium | Website Critical | Lost Sales Critical | Word is crazed students plan an attack later this year Certain | High | A defense in depth strategy along with modern best practices for administrative controls |
| Theft/Loss of sensitive data High | Information improperly stored Low | Proprietary Customer / Supplier Information Critical | Loss of Partner trust and competitive advantage Critical | Could be a target in anticipated attack High | High | Ensure back-ups are maintained in case of accidental deletion. Use encryption for sensitive data at rest |

Types of attacks to watch for:

* Buffer overflow
* Memory leak
* XSS attacks
* DoS/DDoS (Not permitted)
* SQL Injection

Risk mitigation techniques:

* Ensure software is fully updated
* Load open-source security tools
* Use proper secure coding principles for any scripts and HTML
* Load balancing (not possible for this exercise)
* IP Filtering

**Works Cited**

Guta, Michael. “Wow! Small Retail Businesses Hire Nearly 40% of All Retail Employees”, *Small Business Trends.* [www.smallbiztrends.com/2019/07/2019-retail-statistics.html](http://www.smallbiztrends.com/2019/07/2019-retail-statistics.html). Accessed 30 September 2021

Sotnikov, Ilia. “How to Perform IT Risk Assessment”, *Netwrix Blog*. [www.blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/#How\_to\_perform\_a\_security\_risk\_assessment](http://www.blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/#How_to_perform_a_security_risk_assessment). Accessed 30 September 2021

Overby, et al. “What is an SLA? Best practices for service-level agreements”. *CIO*, [www.cio.com/article/2438284/outsourcing-sla-definitions-and-solutions.html](http://www.cio.com/article/2438284/outsourcing-sla-definitions-and-solutions.html). Accessed 1 October 2021.