CSS 3XX Winter 2021
March 9, 2021

# Organizational Risk Measurement Model for Expedia

Expedia is one of the leading purveyors of online travel services including hotels, car rentals, air travel, and cruises. Their operations are fully online (no brick-and-mortar) and they are a transactional entity between travel providers (airlines, hotels, etc.) and consumers. Expedia's online nature and large organization make it vulnerable to numerous threats that can impact their profit margin. These threats can include abusive fraud utilizing the company's payment system and stolen credit cards, employees who may feel vengeful or wish to damage Expedia over personal issues with the company, or criminal syndicates initiating a DDoS attack for notoriety and ransom payment. For each of these threats, the vulnerabilities making them possible are examined along with the troublesome nature of patching the exploits, mainly rooted in the net benefits Expedia must consider if such patches might hinder company efficiency and market exposure. After vulnerabilities are considered, a risk model is offered that is applicable to Expedia's situation and market model, providing the ability to assess the urgency of the company's potential risks and any paths that must be taken to mitigate, transfer, or accept them.

The most common threat faced by Expedia and its subsidiaries is that of individuals seeking to gain advantage by utilizing the services through fraudulently obtained yet usable credit/debit cards and loyalty points. These individuals are increasingly common and sophisticated, particularly as Expedia's operations expand to the developing world, where most of these attackers originate from. The defrauder's typical aim is short-term advantage by avoiding paying for a legitimate travel service offered by Expedia while still reaping the benefits. Such threats do not constitute the potential for large scale *instantaneous* damage but instead put severe strain on the company's services *over time* if ignored.

Vulnerabilities allowing a fraud threat are found in Expedia's web architecture. Transaction code ineffectively validating illegal reward points, and lack of stolen credit card checking allows hackers easy opportunity to exploit the website's payment system (digital shadows, 2020). Relaxed verification permitting such exploits may be intentional for ease of access on the customer's part; however this ease of access allows these loopholes to be exploited by defrauders avoiding any manual verification. This

threat could be prevented by giving a call to the customer to confirm their identity or another verification process through email or texting before approving serious transactions. Any small amount of profit from ease of purchase should be weighed against costs lost to fraud that could be recouped by Expedia if such a strategy were pursued.

A more singular threat posed to the organization is the threat of an insider (employee) of the company using privileged knowledge for personal financial gain or even as a retaliatory measure against the business itself. Although relatively uncommon, this has been demonstrated to be possible through intercepting confidential information passed thru email by management (CNN, 2016). If purposely leaked, such insiders may intend to affect share values or damage brand reputation, as well as cause discord within the company. The typical rationale for such actors usually includes revenge against perceived ills made on them by coworkers or high-ups.

Vulnerabilities that could induce an insider to damage the business can include lax internal data handling procedures, ineffective employee policies, and lack of proper access control and authorization. It is particularly hard to combat abuse of previously provided authorization to employees if they turn rogue; if the employee's data access is not compartmentalized to his direct position, it may provide them an opportunity to do damage beyond their department. Once again, Expedia must weigh a trade-off: employee flexibility versus stringent oversight that may hinder job performance. Additionally, with inadequate legal consequences in an employment contract, an insider may still deem any civil liabilities worth the damage they may be able to inflict upon the company. Beyond normal legal discouragement, proper logging and monitoring can be used to prevent harmful employee behavior described above by making it easier to quickly identify anomalous data downloads, deletions, or alterations within the company network. If such checks are not in place, an Insider will feel emboldened in his/her ability to do damage whilst avoiding consequences and staying undetected, opening up the possibility of even further attacks in the future.

DDoS (Distributed-Denial-of-Service) attacks are another threat for Expedia. Due to a dependence on its primary and subsidiary websites to facilitate communications and purchases from customers, Expedia opens itself up to damage from such an attack if any breakdown of normal website functionality is evident to customers. An attacker directing a DDoS attack on Expedia may have multiple motives: merely causing general mayhem for publicity, being paid for corporate sabotage from foreign competitors, or a

singular financial benefit if the targeted website is judged willing enough to pay in order to prevent an imminent attack (NYU, 2020).

Vulnerabilities to a DDoS attack for Expedia would include insufficient server capabilities and system configuration to handle a sudden flood of traffic, lacking a firewall to block disruptive connection requests, or insufficient barring of dangerous IP ranges. Although Expedia may implement controls like a wide-ranging firewall on specific countries' IP ranges, this becomes more and more unfeasible as their business expands into the developing world. Capping automated requests on the website to only a level usable by a normal human may impact their bottom line as web crawlers and search engines are unable to stay up to date with the website, or the API becomes constrained for partnered websites. A firewall implementation against known compromised connections might miss botnets that have been formed only recently. Another new and related issue is that of an internal DDoS attack where the companies own device connections are hijacked back at itself (perimeter 81, 2020), a situation increasingly plausible as companies implement insecure products as part of the economy's shift towards the Internet of Things.

If any of the above threats successfully manage to exploit the vulnerabilities, the company's operations would be at risk in multiple areas. Normal finances and profit margin may be reduced, sensitive information may be publicized maliciously, there may be downtime of systems crucial to Expedia's business model, or even damage to Expedia's brand and reputation. Ensuring that these areas are not at risk is critical to Expedia remaining competitive and dominant in the market. A method of measuring this risk is provided as follows based on a likelihood versus consequence model from SRMAM:

# Cyber-Security Risk Matrix

Adapted from www.srmam.com

| | Negative Consequence | | | | |
|---|---|---|---|---|---|
| **CAPABILITY** | Minor skills reduction at individual or workgroup level | Minor adverse impact on organizational capability | Unavailability of core skills that substantially affects services | Unavailability of critical skills or personnel that has a major impact | Protracted unavailability of critical skills/people has catastrophic impact on outcomes |
| **FINANCES** | <10% adverse impact on the organisations profit or operating budget | >10% adverse impact on the organisations profit or operating budget | >50% adverse impact on the organisations profit or operating budget | >100% adverse impact on the organisations profit or operating budget | >200% adverse impact on the organisations profit or operating budget |
| **PEOPLE** | A 'near miss' or minor injury | Absences from work for up to a week, possibly requiring medical treatment | Hospitalisation required due to serious injury | Fatality or multiple major injuries | Multiple fatalities |
| **INFORMATION** | Compromise of information otherwise available in the public domain | Minor compromise of sensitive information sensitive | Moderate compromise of sensitive or classified information | Major compromise of sensitive or classified information pertaining to key organizational objectives | Catastrophic compromise of sensitive or classified information pertaining to key organizational objectives |
| **PROPERTY** | Insignificant adverse impact to organizational assets (<2%) | Minor impact on organizational assets (2% to 25% of assets/value) | Moderate impact on organizational assets (26% to 50% of assets/value) | Major impact on organizational assets (51% to 75% of assets/value) | Catastrophic impact on organizational assets (>75% of assets/value) |
| **BRAND/ REPUTATION** | Adverse local mention in media Quickly forgotten Self-improvement review required | Scrutiny by Executive, internal committees or internal audit to prevent escalation | Scrutiny required by external committees, auditors, ASIC etc | Intense public, political and media scrutiny Eg: front page headlines, TV, etc | Government or Legal inquiry or sustained adverse national/international media |
| **SYSTEMS** | Minimal impact on non-core business operations which can be dealt with by routine operations | Business delays and/or quality which be dealt with at operational level | Reduced performance such that targets are not met requiring significant review or changed ways of operations | Breakdown of key activities reduce business performance, create service delays, client dissatisfaction, costs, legislative breaches | Critical business failure, preventing core activities from being performed which threatens survival of the organization or project |
| **OBJECTIVES** | Minimal impact on organisational outcomes or strategies | Some adverse impact on organisational outcomes or strategies but can be managed by routine procedures | Moderate adverse impact on organisational outcomes or strategies | Major adverse impact on organisational outcomes or strategies | Increased barriers or failure of strategy, likely to cause catastrophic impact on objectives |

| Likelihood | Qualitative Likelihood | Quantitative Likelihood (% Probability) | | | Insignificant | Minor | Moderate | Major | Catastrophic |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 | 4 | 5 |
| ↑ | Is expected to occur in most circumstances | Has occurred on an annual basis or circumstances exist that will cause it to happen on an annual basis. (>99% Probability) | 5 | Almost Certain | 6 | 7 | 8 | 9 | 10 |
| | Will probably occur in most circumstances | Has occurred within the last 3 years or has occurred recently in similar organizations or circumstances exist that will cause it to happen in the next few years. (>66% probability) | 4 | Likely | 5 | 6 | 7 | 8 | 9 |
| | Might occur at some time | Has occurred at least once in this company or similar companies (>33% probability) | 3 | Possible | 4 | 5 | 6 | 7 | 8 |
| | Could occur at some time | Has never occurred in this company but has occurred infrequently in other similar companies (<33% probability) | 2 | Unlikely | 3 | 4 | 5 | 6 | 7 |
| ↓ | May occur only in exceptional circumstances | Is possible but has not occurred to date in this company or any similar company. (<1% probability) | 1 | Rare | 2 | 3 | 4 | 5 | 6 |

## Management of Negative Risks

| | |
|---|---|
| EXTREME (E) | Immediate action by Executive management and detailed planning |
| HIGH (H) | High risk, senior management attention needed |
| MEDIUM (M) | Management responsibility must be specified |
| LOW (L) | Managed by routine procedures |

Utilizing this model, Expedia's risks can be explicitly categorized into areas ranging in likelihood from 'Rare' to 'Almost Certain', and consequences are organized in degree from 'Insignificant' to 'Catastrophic'. As previously mentioned, the threat of credit and reward fraud against Expedia is quite common – 'Almost Certain' – yet the impact of this fraud is generally 'Insignificant' for the company's profit margins; Expedia has generally chosen to *accept* the risk of fraud due to its medium risk nature. However, less predictable threats may vary in their risk measurement effect depending on an attacker's rationale, goals, and tools which may be more intense even if the 'threat' is the same. This can be shown by the variance of consequence in Insider and DDoS attacks.

Due to Expedia's history of already having an Insider who intercepted emails from management due to abused IT credentials for personal profit, the threat of an Insider lands squarely in the 'Possible' category since it has been demonstrated to have occurred at least once already (CNN, 2016). In this previous scenario, the bad actor did not intend to specifically damage the company but rather simply used his privileges for personal gain, meaning the incident's consequence was 'Insignificant'. Note that in this case, the risk of the incident was *transferred* to the SEC who forced the hacker to repay Expedia for damages. This incident fell into the green sector of the matrix, of 'LOW RISK', and was predictably managed by routine procedures in the company as the incident was resolved. However, if an insider was bent on doing damage to the company as discussed previously for personal revenge, the chance of such damage may remain in the 'Possible' likelihood yet the consequence of such an attack would undoubtedly be 'Major' or 'Catastrophic' for the company depending on the insider's access and credentials. This would be considered a 'HIGH RISK' scenario where senior management would need to be involved.

In the realm of DDoS attacks, due to the varying nature of a threat's goals, the severity and sophistication may vary from a simple 'MEDIUM RISK' situation where a small botnet is utilized to cause a temporary disruption of website service to a 'HIGH RISK' attack where Expedia's systems are unable to operate for multiple days at a time due to a huge botnet targeting vulnerable links in Expedia's public server interface. The chance of these DDoS attacks occurring would best fit within the 'Likely' category, yet their damage could range from 'MEDIUM RISK' all the way to 'EXTREME RISK' if Expedia's services and websites were rendered inoperable for days on end. This demonstrates how a single threat (that of a DDoS attack) can not always be limited to a single cell in a risk measurement model but may occupy

multiple potential risks and likelihoods simultaneously. Due to the unpredictable nature of this threat, the best solution is to *mitigate* any risk preemptively by building up effective firewalls and resources to withstand a DDoS attack while maintaining service to customers.

The threats and risks above are not unique to Expedia; most e-commerce sites are forced to defend against fraud, employee behavior, and DDoS attacks. However, the increased likelihood of Expedia being targeted over smaller and lesser known e-commerce companies can be attributed to the lucrative nature of vacation and travel services offered by the company, their business success in the last few years, and the troves of data the company compiles and maintains. Threats are varied: some common (such as fraudsters), some particularly rare (the Insider), and others extremely sophisticated (DDoS attackers). Although fixes exist for many of the vulnerabilities commonly exploited by these threats, instituting them must be taken with a balanced approach to avoid complicating operations, encumbering customer experience, or flagging too many false positives. In assessing risks, Expedia may choose to accept risk that is predictable such as fraud, transfer risk as seen in handing over responsibility for an Insider attack to the government, or mitigate risk that the company deems reducible such as in the case of DDoS attacks

REFERENCES

CNN (2016) Expedia IT guy made $300,000 by hacking own execs.
Retrieved from
https://money.cnn.com/2016/12/05/technology/expedia-hack-insider-trading-sec/
New York University (2020) The Rise of DDoS Ransom Attacks – How to Prevent and Respond
Retrieved from
https://wp.nyu.edu/compliance_enforcement/2020/12/23/the-rise-of-ddos-ransom-attacks-how-to-prevent-and-respond/
digital shadows (2020) Dark Web Travel Agencies: Take a Trip On The Dark Side
Retrieved from
https://www.digitalshadows.com/blog-and-research/dark-web-travel-agencies-take-a-trip-on-the-dark-side/
perimeter 81 (2020) “Increasing DDoS Sophistication” in The Psychology Behind DDoS Attacks
Retrieved from
https://www.perimeter81.com/blog/network/the-psychology-behind-ddos-attacks/