

Computer Systems

Security Foundations

Week 1: Introduction to Information Security

Aidan Polivka

Feb 10, 2024

Table of Contents

Project Outline and Requirements (Week 1)	3
Organization Description.....	3
Proposed Migration Architecture	3
Project Requirements	4
Introduction to Information Security (Week 1).....	5
The Need for Information Security	5
Why Ensure Compliance with Sarbanes-Oxley and PCI DSS?	5
Access Challenges for Consultants.....	5
Security Assessment (Week 2)	6
Access Controls and Security Mechanisms (Week 3).....	9
Software and Database Security (Week 4).....	10
Network Security (Week 5)	11

Project Outline and Requirements (Week 1)

Organization Description

Heartland Escapes is a chain of bookstores in Southeastern Nebraska. They started small with two stores in the capital city Lincoln, but due to successful social media marketing campaigns they have expanded to two other cities: Omaha, and Grand Island. These two new locations have continued to show success and deliver significant revenue. What sets Heartland Escapes apart from other bookstores is their use of events. They host several events throughout the year, including author meet & greets, scary story readings for kids on Halloween, fun Easter and Saint Patrick's Day parties, summer book reading for kids, etc. These events are well advertised and well attended because of Heartland Escapes social media presence. Because of Heartland Escapes quick growth, they've engaged in a modernization effort to migrate their technological infrastructure to an Azure hosted cloud environment. Their on-premises system was stood up in 2009 and hasn't received much of an upgrade over time, so they've contracted us as security experts to assess the security of their proposed migration effort.

Proposed Migration Architecture

The contractors working on the migrated architecture have a thorough document on how they plan to build this new infrastructure. They have taken security measures into account to the best of their ability, but it's our job to evaluate the planned infrastructure and provide more detailed suggestions as to how this infrastructure can achieve the desired level of security by Heartland Escapes.

"I suggest configuring Azure into two resource groups: one for data and infrastructure, and the other for applications. All resources should be in the us central region. In the application storage container, there will be three app services: one for the Point-of-Sale web application, one for the Inventory Service, and one for the public website. Azure App Services are like containers with a base operating system. In this case, I recommend running all services on a Windows system for simplicity. The app services would use the Premium v3 P1V3 hardware tier, which includes two vCPUs and 8 GB of RAM per instance, with the ability to scale up to 30 instances. In the data and infrastructure group, there would be an Azure SQL Server hosting both databases, and a virtual network (vNet) that manages firewall rules and security. A vNet Gateway would allow users to access the system via VPN. The public website would be the only part of the system outside of the vNet, accessible only through the gateway. The public website's IP address would also have access." (Polivka, 2023)

Later in the document, the author goes on to discuss the need for Azure Active Directory and role base security, which is an Azure component missing from this high-level proposal.

Project Requirements

Because their on-premises system was set up well before network and system security was standardized as a top priority, there are a lot of gaps in the security of their infrastructure. As they migrate into this new infrastructure, they want to prioritize security modernization as well. An important note is that Heartland Escapes transmits customer banking information for online transactions, so they must fall into compliance with the Payment Card Industry Data Security Standard (PCI DSS). They also would like to be able to store customer banking information in the future to set up an e-commerce website, which is even more reason to follow PCI DSS. For an additional twist, after the migration effort has taken place Heartland Escapes wants to go public and release a new IPO. So, not only do we need to ensure compliance with PCI DSS, but also the Sarbanes-Oxley Act regulations.

Our key goals in this security assessment are as follows:

- Evaluate requirements for the PCI DSS and Sarbanes-Oxley and ensure Heartland Escapes security policies meet these requirements.
- Evaluate the security risks of the proposed environment.
- Evaluate access control methods that are proposed, identify alternative controls, and provide our own proposal as security experts.
- Evaluate the need for controls to better protect data both at rest and in transit.
- Develop or redesign a secure network solution.

Introduction to Information Security (Week 1)

To perform what is required of us by Heartland Escapes, we must first review the proposed infrastructure and security model to ensure compliance with the Sarbanes-Oxley act and PCI DSS. We also need to know what risks are presented by remote hosting of the organization's system, the challenges that we as consultants will face for access, and the challenges that apply due to Heartland Escape's desire to take an IPO.

The Need for Information Security

The need for information security is clear. If Heartland Escapes wants to go public without risking fines for failing compliance, they need to secure user's information. That reason is strictly for the sake of Heartland Escapes, it's also a major risk to not secure user information for the sake of Heartland Escapes customers. If user data is leaked, a Heartland Escapes is sure to lose customers and reputation while hurting the consumers that keep their business running and the communities that built their business.

Why Ensure Compliance with Sarbanes-Oxley and PCI DSS?

PCI DSS is required guidelines for institutions interacting with customer banking information. Since Heartland Escapes transmits and will eventually store user banking data, they must comply with these guidelines or risk fines. Because Heartland Escapes plans to go public, they will be required to comply with regulations defined by the Sarbanes-Oxley act. Further discussion around the details of following these compliance regulations must be had.

Access Challenges for Consultants

Because Heartland Escapes' new environment is hosted in the cloud, we as consultants have no need to access on premises systems or to work on-site. This is beneficial to us so we can continue to work from home, or the home office. However, if they have sufficient access controls, we might run into roadblocks with permissions at the start of the audit process.

Security Assessment (Week 2)

Assets

As it stands, Heartland Escapes has several assets to protect. Thankfully, a lot of the work needed to identify these assets has already been completed by the teams working on the migration effort. They've already identified these assets from the on-premises machine because their goal is to segment them out into Azure controlled resources.

For data assets, Heartland Escapes has two databases: their accounting database and their inventory database. The data stored in the accounting database right now is strictly to track payments and charges for taxes. Eventually when they convert their system to an ecommerce website, they may end up storing customer account information. It's important that we consider this future goal when assessing the security around the database, because it'll be valuable information for the modernization effort. The inventory database is only for operations. Here they track the individual store's inventory, and this data is served to multiple applications for different purposes.

Heartland Escapes also has a few application assets, their public website, a home-grown point-of-sale system, and their inventory API. The only application that is accessible from outside the network is the public website, everything else is accessible by either the public website, or from within the network. All these applications are valuable and contain protected technology and code that should be safe guarded from prying eyes.

Network Segregation

Heartland escapes current system does not have any form of network segregation for their assets. This is generally a risk for multiple reasons:

Enlarged Attack Area. Without network segregation, all of Heartland Escapes assets are susceptible to a single attack on their server. It's the same principle of the adage, "putting all your eggs in one basket". You run the risk of something happening to that one basket, and all your eggs getting ruined at once. This is a precursor to what's called "lateral movement". If the bad actor has access to one service within your network, then they have easier access to elevate their own permissions, and access more critical parts of the network.

Data Integrity & Regulatory Compliance. It is typically poor practice to store highly sensitive data with insensitive data, specifically if they aren't expected to be used at the same time. Depending on the use case for said data, there may be standardized compliance guidelines around data storage that require network segmentation. This can be costly if not upheld.

Monitoring and Detection & Incident Response. Monitoring network traffic to a congested network hosting multiple business domains can be complicated. It is much simpler to monitor network traffic to a more modularized network ecosystem, which makes finding anomalies in such an

environment easier. As a result, if you're more able to monitor and detect network anomalies, then you'd be better able to respond to incidents. Having a tightly coupled network environment without any segregation of concerns can result in slow and complex incident responses.

Least Privilege Principle. The least privilege principle expects that only elements that need access to an asset, should have access to an asset. By having all resources on the same network, fundamentally this principle is broken, and causes a lot of risk.

Because our consulting firm's role on the project at this moment is strictly to analyze the proposed migration effort, we don't have any need to access the on-premises machine, or any of the hosted data or applications. Once the migration effort has taken flight with our assessment and suggestions in place, we can perform a secondary audit of their cloud hosted infrastructure from the comfort of our own homes, or the corporate office. If we did need to remote into the on-premises server, this would pose an additional risk to their system. Any additional holes we poke into their firewall, and any additional access points to their network can cause unnecessary risk.

Risk Assessment Strategy

Our game plan for analyzing Heartland Escapes ecosystem for risks is simple. We will analyze each service's vertical slice of functionality within the network. To elaborate, we'll take an individual service (starting with the inventory service since it is central to the rest of the system), and evaluate the service itself, it's positioning within the network, the database that the service is married to, and the network protocols used to communicate to internal and external structures. Once each service is evaluated, we'll look at the larger system and perform a high-level horizontal analysis of the network itself, and the data segregation.

Any found risk will have its own assessment. The most important structure to understand about each risk assessment is the risk level. We will use a 5 x 5 matrix to communicate the threat level of each risk. The x axis is 1-5 likelihood that this risk would be exploited, and the y axis is 1-5 risk severity. This heat map is a great way to determine what the threat level is and explain to Heartland Escapes the impact of the found risk. Here is a list of the expected contents of each assessment: risk scenario, identification date, existing security controls, current risk level, proposed treatment plan(s), progress status, residual risk (what is the risk level after each potential treatment), and the risk owner. (Cobb, 2024)

Risk Mitigation Options

As part of the risk assessment, a treatment plan must be chosen to propose to Heartland Escapes. What actions are taken to mitigate the risk at the end of the day is the decision of Heartland Escapes. If they want the expense of making code changes, or paying for third party services to mitigate risks, that is their prerogative. Our job is to offer *potential* resolution options. These resolution options can come in one of four different varieties, or a combination of any of these four varieties:

Avoidance. At this point, avoidance is an option we'll seldom suggest to Heartland Escapes, because their goal is to get our input on their modernization effort. However, this scenario is when the technology that poses the risk isn't valuable enough to fix. If it's deprecated, or unused, then the proposal could be for Heartland Escapes to discontinue use of the technology.

Transfer. This may be a commonly proposed option. Rather than suggesting code changes, we may propose that Heartland Escapes takes advantage of third-party software to mitigate an identified risk. For example, Azure (which happens to be the platform Heartland Escapes is migrating to) has tools for protecting against DDoS attacks. If it's found that Heartland Escapes' public website is susceptible to such attacks, it may be more worthwhile to suggest utilizing Azure's technologies over making code changes. Or we could prevent this attack from multiple angles by both *transferring* the mitigation effort and *reducing* the risk ourselves with code changes like rate-limiting requests.

Reduce. The third option is to reduce the risk by making explicit changes. Carrying forward the example of a DDoS attack, we could choose to *reduce* the ability of bad actors to perform such an attack by rate limiting requests from IP addresses to the public website. (Cobb, 2024)

Acceptance. The final option is to accept the risk. The only scenario in which we would ever suggest accepting a risk is if it's been determined that the risk threat is minuscule, and the cost to mitigate the risk through another means is more expensive than it's worth. Accepting a risk *is* a risk within itself and should be suggested with caution.

Access Controls and Security Mechanisms (Week 3)

TBD

Software and Database Security (Week 4)

TBD

Network Security (Week 5)

TBD

References

Polivka, A. D. (2023). Modernizing “Heartland Escapes” to a Cloud-Hosted Infrastructure.

Cobb, M. (2024, January 18). How to perform a cybersecurity risk assessment in 5 steps: TechTarget. TechTarget | Security. <https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step>