Session 4 Assignment(Research and Written Report)

Identity Management Challenges:

implementing identity management (IDM) solutions is essential for organizations to manage user identities, control access to resources, and protect sensitive data. However, this process comes with several challenges that can make effective IDM implementation complex. Some of the most common challenges organizations face include:

1. Discuss common challenges organizations face in implementing identity management solutions, such as managing access rights, scaling, and integrating with existing systems.

1. Managing Access Rights:

Complexity of Access Controls: Organizations often have diverse roles and access needs, making it challenging to define and manage access rights. Each user must have the right level of access to do their job without having excessive permissions, which can create security risks.

Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC): Setting up and maintaining access controls is complex, especially when roles change frequently, or when employees have unique access requirements. Managing these frameworks can be time-consuming and challenging to scale effectively.

3. Scalability

Growing User Base: As organizations expand, the number of users and devices grows, making it harder to manage and scale IDM systems. Scaling requires solutions capable of handling high volumes of authentication requests efficiently and securely.

Handling Peak Usage: Organizations often experience peak periods when many users need access at once (e.g., during a product launch or end-of-month reporting). IDM solutions must be scalable to handle such demand without compromising performance.

2. Integration with Existing Systems

Legacy Systems Compatibility: Many organizations rely on older systems that may not be compatible with modern IDM solutions. Integrating these systems often requires custom solutions or middleware, increasing implementation complexity.

Cloud and Hybrid Environments: Organizations increasingly operate in multi-cloud or hybrid environments, requiring IDM solutions that can integrate seamlessly across these diverse environments. Achieving consistent identity management policies across all platforms is often challenging.

2. Provide examples of identity-related security incidents (e.g., account takeovers) and explain how they could have been prevented with proper identity management.

When was the Marriott breach?

On September 8, 2018, an internal security tool flagged as suspicious an attempt to access the internal guest reservation database for Marriott's Starwood brands, which include the Westin, Sheraton, St. Regis, and W hotels. This prompted an internal investigation that determined, through a forensics process that Marriott has not discussed in detail, that the Starwood network had been compromised sometime in 2014 — back when Starwood had been a separate company. Marriott purchased Starwood in 2016, but nearly two years later, the former Starwood hotels hadn't been migrated to Marriott's own reservation system and were still using IT infrastructure inherited from Starwood, an important factor that we'll revisit in more detail later.

In their investigation, Marriott found data that the attackers had encrypted and attempted (probably successfully) to remove from the Starwood systems. By November, they had managed to decrypt that data and discovered that it included information from up to 500 million guest records, though those undoubtedly include duplicate records or multiple records pertaining to individual guests. Many of the records include extremely sensitive information like credit card and passport numbers. Now aware of the severity of the breach, Marriott released a statement on November 30, 2018, outlining the basics we've described here.

What caused the Marriott data breach?

Marriott first became aware that they'd been hacked when a security tool flagged an unusual database query. (The tool was actually monitored by Accenture, who had been running IT and infosecurity for Starwood before the merger and continued to do for the legacy network afterwards.) The database query was made by a user with administrator privileges, but analysis quickly revealed that the person to whom that account was assigned was not the one who made the query; someone else had managed to take control of account.

Investigators began scouring the system for clues, and discovered a Remote Access Trojan (RAT) along with MimiKatz, a tool for sniffing out username/password combos in system memory. Together, these two tools could have given the attackers control of the administrator account. It's not clear how the RAT was placed onto the Starwood server, but such Trojans are often downloaded from phishing emails, and it's reasonable to guess that might've been the case here.

But lurking behind these specific attack vectors lay a series of cultural and business factors that we might label the root cause of the breach. What stands out here is not the attack's success in breaching Starwood's systems — most security experts today believe it's almost impossible to keep all attackers at bay all the time — but rather that the attack went undetected for four years. Starwood did not have the best security culture before its acquisition by Marriott; the Wall Street Journal reported that Starwood employees perennially found the reservation system

difficult to secure, and in fact a different attacker breached the system in 2015 and wasn't detected for eight months. Then, after Marriott acquired Starwood in September 2016, most of Starwood's corporate staff, including those managing information technology and security, were laid off. That sort of payroll cutting is exactly what produces the "synergies" and higher profits that drive these sorts of mergers in the first place, of course, but Marriott was nowhere close to ready to book guests at its thousands of newly acquired hotels with its own in-house reservation system, and so Starwood's old system limped on, zombie-like, infected with malware, breached by hackers, and without much by way of continuity of care, for another two years before the breach was finally discovered.

What was the impact of the Marriott breach?

At one level, the Marriott breach was potentially catastrophic: hundreds of millions of people had their passport and credit card numbers stolen, which could have disastrous personal impacts. The credit card number aspects are particularly worrying, and were made possible by yet another security failing on Marriott's part: while the credit card numbers were stored in encrypted form, the encryption keys were stored on the same server, and were also apparently scooped up in the breach. As for the passport numbers, while some were encrypted, the majority were simply saved in the clear.

But the breach in fact does not seem to have had the damaging impact on Starwood customers that it could have. That may seem strange, and to understand the reason for it, we need to answer a couple more questions: who breached Marriott, and why**.**

Who hacked Marriott and why?

The Post's and Times's sources had access to more data about the hack than has been made public, and say that the code and attack patterns used match up with techniques employed by state-sponsored Chinese hackers; the attackers used a cloud-hosting space frequently used by Chinese hackers, for instance. (The involvement of U.S. intelligence service in the investigation and the sensitive nature of the attack probably explains why not much by way of technical details has been released.) Another clue that this breach is part of a government attack rather than mere cybercriminals is the fact that none of those millions of valuable records have ended up for sale on the dark web; this wasn't a mere plundering raid.

What would the motivation for the attack be, then? The government sources speculate that it was part of a broader Chinese effort to acquire massive amounts of data on American government employees and intelligence officers; Marriott is the top hotel provider for the U.S. government and military. The stolen passport numbers in particular could be used to track movements around the world. The breach of the Office of Personnel Management's systems, which similarly resulted in millions of individuals having their data stolen but none of that data ending up on the dark web or being used for fraud, was probably part of the same campaign. The larger goal is to create a data lake of information on American government employees and agents that big data techniques can be used to analyze

How did Marriott respond to the breach?

Perhaps because there seems to be no immediate threat of the stolen data being used for conventional fraud, Marriott has not gone out of its way to compensate any of its customers whose data was stolen. The New York Times quotes a Marriott spokesperson as saying the company would pay the replacement cost for a passport with a new number or cover credit card expenses "if fraud has taken place." While the potential damage from personal data now stored with Chinese intelligence is in theory profound, it's difficult to quantify, especially for individuals.

What did the Marriott data breach cost?

That doesn't mean the company's getting away scot free, however. As of March 2019, the company had incurred $28 million in expenses related to breach — and yet that only lowered the company's bottom line by $3 million. By May, the company had cut its losses to a mere $1 million. How? Cyberinsurance, which covered much of the initial costs associated with the crisis. Insurance against cyberattacks is a relatively new offering, but it seems to have paid off for Marriott.

And indeed, in July of 2019 a much harsher blow landed on the company. The UK's Information Commissioner's Office (ICO) levied a fine of £99 million — more than $120 million — for violating British citizens' privacy rights under the GDPR. (The GDPR is an EU law, but still applies to Britain as Brexit has yet to go through.) Again, the ICO specifically cited Marriott's failure to do due diligence on Starwood's IT infrastructure as an explanation as to why Marriott was being punished for Starwood's mistakes. The massive fine may only be the beginning, as other jurisdictions could also look to punish the company for its lapses.

how they could have been prevented with proper identity management.

1. Implement Strong Authentication Controls: The breach likely stemmed from unauthorized access to Marriott's systems. Using multi-factor authentication (MFA) for all employees, especially for privileged accounts, could have added an extra layer of security, making it harder for attackers to access sensitive systems even if passwords were compromised.

2. Regular Access Audits and Reviews: By conducting regular audits of user permissions, Marriott could have identified unusual patterns or unauthorized access sooner. Access audits help ensure that only those who need certain data for their roles can access it, limiting exposure in the event of a compromise.

3. Role-Based Access Control (RBAC): Ensuring strict, role-based access control policies limits access to sensitive data based on employees' roles. If Marriott had implemented granular access controls, only specific users (like those in finance or customer service) would access guest data, reducing the risk of widespread exposure.

4. Privileged Access Management (PAM): Privileged accounts typically have more extensive access rights, making them high-value targets. Using PAM would have helped Marriott secure these accounts through stricter access control, session monitoring, and advanced logging. Any suspicious activity on privileged accounts would be quickly flagged and investigated.

5. Data Encryption and Tokenization: Encrypting sensitive data, such as personal details of guests, both in transit and at rest, can prevent data misuse even if unauthorized access occurs. Tokenization replaces sensitive data with non-sensitive equivalents, meaning even if data is accessed, it has minimal value outside the original system.

6. Continuous Monitoring and Anomaly Detection: Proactively monitoring network traffic and user behavior would enable Marriott to detect unusual patterns, such as an account accessing data outside of regular hours or from unfamiliar locations. Early detection would have enabled faster responses to potential breaches.

7. Centralized Identity Governance: Marriott could have used a centralized IAM system to manage and monitor user access across all its properties. This would streamline the process of creating, modifying, and removing access for employees across all locations, helping ensure that terminated employees or contractors no longer have access to the system.

8. Employee Training and Awareness: Marriott could have emphasized cybersecurity awareness, training employees on IAM best practices, password hygiene, and phishing recognition. Employees would be better prepared to recognize potential threats and maintain security standards.

1. Identity and Access Management Lab: