HealthCo[1]

At 11pm on a Sunday, a world-renown surgeon backed his Ford Super Duty F-450 through the glass doors of an entrance at one of HealthCo's hospitals. He had received an urgent call to do a lifesaving surgery on an emergency patient. He arrived at the nearest entrance within five minutes, only to be stopped by a badge access that did not work. He had no time to call IT and wait for the access problem to be resolved. His access to the building was a life and death matter. The surgeon did not hesitate to force his way through the entrance door. After completing the surgery and saving the patient, he returned to the truck and left a note for the hospital management on the windshield wiper: "You owe me a new truck!"

This was the apex of mounting identity and access management (IAM) problems at HealthCo. While everyone had experienced some sort of IAM problem, until this incident, IAM was relegated to a technical issue. The surgeon not only saved the patient but also elevated the IAM problems to the agenda of HealthCo's top management team (TMT) and board of directors (BoD). Was it time to retire HealthCo's home-grown, legacy IAM and replace it with a modern, enterprise-grade IAM solution?

HealthCo had survived the challenges of the pandemic but it was not yet off-the-hook of many financial challenges. Investment into a modern IAM would likely require significant capital expenditure (CapEx) and or operating expenditure (OpEx). As a large health system, HealthCo was already spending hundreds of millions of dollars into IT each year. But, at any given time, it had more IT investment proposals than its limited IT budget could afford. Any new IT investment proposal had to compete not only with dozens of other IT investment proposals but also with medical technology investment proposals. For instance, the TMT and the BoD were currently evaluating a CapEx into MRI machine modernization. MRI machines in many member hospitals of HealthCo had become antiquated. They were frequently breaking down and causing disruptions to care services and leading to the loss of patient revenues. Many HealthCo patients started switching to rival hospitals citing the MRI problems. An investment into a modern, high-end MRI machine required a CapEx of $3 million per machine. HealthCo would need to urgently modernize MRI machines of at least ten of its 97 member hospitals. Champions of MRI modernization quantified the business case and argued that the modernization of ten MRI machines would have a net present value (NPV) of $25.68 Million and a Return on Investment (ROI) of 100% over the next five years. Knowing that they would be competing up against such alternative investment proposals, champions of the IAM investment wondered whether the IAM investment's NPV and ROI metrics would be comparable or better. While the surgeon's ordeal helped the TMT and the BoD realize that IAM can affect patient care, the impact of an IAM investment on patient care was not as obvious as the impact of an MRI modernization. Thus the champions of the IAM investment also wondered how they could supplement their quantitative business case with qualitative arguments on how IAM could improve quality of care and patient outcomes.

---

[1] This case is prepared by Dr. Hüseyin Tanriverdi of the University of Texas at Austin for educational classroom use only. It also received significant input from Collin Perry, a cybersecurity expert. The case provides students with an opportunity to apply their valuation skills and knowledge to estimate costs, benefits, and risks of HealthCo's investment into a cybersecurity and privacy solution. HealthCo is a fictitious company. The case makes reference to a real vendor's (SailPoint) solutions, but the functionality, pricing models, and pricing information on SailPoint's solutions are modified to create decision scenarios and dilemmas to maximize the learning objectives. If reader is interested for doing this exercise for a real company, the specific functionality, pricing model, and parameters values need to be updated in collaboration with the vendor and the company.

BACKGROUND

HealthCo is among the largest health systems in the U.S. With about 125,000 employees and 2500 contract workers, HealthCo operates 97 hospitals and 235 other healthcare facilities (e.g., nursing homes, senior care centers, urgent care centers and other health and well-being centers) in 32 states across the US. HealthCo's annual patient revenues reached $25Billion in fiscal year ended December 31, 2022.

HealthCo has a social mission of serving underserved patient populations. It aspires to improve the productivity of operations to release cash and use the released cash to provide care to uninsured patients at reduced costs, or free of charge. In 2022, HealthCo was able to achieve $500Million in productivity savings, about 2% of its annual revenue, and allocate it for the care of uninsured patients. Over the next five years, HealthCo aspires to achieve a lot more productivity savings and allocate about 7% of its annual revenues to the care of uninsured patients.

There are a lot of redundancies and inefficiencies in HealthCo's operations due to the organization's rapid growth through mergers and acquisitions. HealthCo came into being through the merger of two hospitals 30 years ago. Since then, HealthCo has aggressively acquired more hospitals, physician practices, nursing homes, senior care centers, urgent care locations, and other healthcare facilities. The stated goal of the acquisitions was to create integrated healthcare delivery systems in HealthCo's patient markets. By offering the full continuum of care, HealthCo aimed to serve as a single stop shop for all healthcare needs of a person from birth to death. However, HealthCo has struggled to achieve this goal primarily due to the lack of a common, enterprise-wide digital platform from which the acquired units could be supported. Each acquired entity requested autonomy to maintain its specialization and talent, and compete effectively with its local rivals. In response, HealthCo had to set up the acquired entities as independent organizational units reporting to HealthCo's corporate center. Each acquired unit joined HealthCo with its own set of IT systems, IT applications, business processes, and data. There were compatibility and interoperability problems among the IT silos of the acquired units. Any cross-unit connections were ad hoc at best. Thus, HealthCo's enterprise-wide IT architecture remained at the "silo" stage, the lowest level of maturity.

HealthCo's governance is mostly decentralized. The units have decision rights over which medical services to offer, how to make deals with health insurance companies, and how to organize and govern their IT applications and clinical and administrative support functions. The corporate center of HealthCo has decision rights only over the lowest common denominator of corporate support functions such as accounting, finance, treasury, tax, HR, IT security, IT infrastructure, and regulatory compliance with relevant laws, regulations, and standards.

HeathCo's TMT and BoD have been aware of the need to embark on a major digital transformation journey to standardize and integrate IT systems of the acquired hospitals. Digital transformation experiences of similar-sized health systems suggested that HealthCo would need at least a decade to complete such a digital transformation. But, HealthCo faced many immediate problems and risks, and it has not been able to afford to wait for the completion of a decade long digital transformation journey. The proliferation of IT application silos already led to very high IT costs and inhibited HealthCo's goal to achieve productivity savings and use the released cash to serve uninsured patients. In addition, IT application silos heightened HealthCo's IT-related risks such as cybersecurity breaches, privacy breaches, operational IT failures, regulatory compliance problems and costs, digital fraud, etc. These risks also made it difficult for HealthCo to find insurance firms willing to

offer cybersecurity liability insurance. HealthCo's cyber insurance premiums kept going up. There was also evidence that some of the digital risks already realized.

CYBERSECURITY RISKS

In each of the past 10 years, HealthCo experienced at least one data breach per year. In the least damaging incident, only one hospital had a patient data breach and leaked 500 patient records. Any breach leaking 500 or more patient records has to be included in the annual "wall of share" for patient data breaches in U.S. hospitals. HealthCo consistently made this wall of shame. The shortcomings of HealthCo's legacy IAM seemed to have played roles in these cybersecurity breaches. In the worst year, there was a breach affecting all hospitals of HealthCo simultaneously. But luckily, HealthCo was able to detect and stop the breach after the leakage of 175,000 patient records. Based on an analyses of the historical data, HealthCo estimates the likelihood of experiencing a data breach in a given year as follows: minimum likelihood of 1%; maximum likelihood of 100%; and most likely 10%. HealthCo also estimates that the impact of a breach on patient records leakage would be as follows: minimum impact: 500 patient records; maximum impact: 3,200,000 records; and mostly likely impact: 175,000 patient records. HealthCo also estimated the potential costs associated with a patient data breach and summarized them in HealthCo's Excel Workbook tab "12. Risk-CyberLossExposure(CLE)."

Caregivers at HealthCo have been spending a lot of time logging on to multiple IT applications multiple times per day. Remembering login credentials for the many IT applications has been challenging. As HealthCo implemented industry best practices for the complexity requirements of passwords, caregivers had faced even more difficulty in securely storing and recalling complex passwords of multiple IT applications. When caregivers forget the complex passwords, there was no self-service functionality in the legacy IAM for resetting the passwords. Caregivers had to call the IT help desk to get their passwords reset manually. Also, caregivers were often called to other units on an emergency basis. They often have to wait until access could be provided to the requesting unit's IT applications and restricted areas. The time caregivers had to spend on such access issues was time taken away from patient care. Although it was against HealthCo's cybersecurity policy, app access problems also forced physicians and nurses to give access rights to physician assistants and nurse assistants so that the assistants could manage the mundane app login and patient data entry tasks on their behalf while the physicians and nurses focused on patient care.

The violations of access policies increased the likelihood and the impact of cybersecurity and privacy breaches. For instance, a member hospital experienced a ransomware attack, and access right violations amplified the impact of the attack. A physician assistant, who was not supposed to have access to critical patient IT applications, were provided access. Hackers targeted phishing e-mails to physician assistants, and unfortunately, this physician assistant fell to one of the attacks. When the physician assistant responded to the phishing e-mail, the hackers gained access to her e-mail account, and using her (excessive) access credentials, they accessed critical patient IT applications and exfiltrated protected health information (PHI) of about 10,000 patients. The exposed PHI included patients' names, demographic information, dates of birth, diagnoses, treatments, medical record numbers, and in some instances, health insurance identification numbers.

Furthermore, when the physician assistant clicked on the malicious link, malware was installed, and it started encrypting IT applications. A message popped up on the infected systems warning that unless the hospital paid a ransom of $1Million within two days, hackers would post the exfiltrated PHI on the dark web. The malware spread quickly to encrypt all systems of the hospital within two hours. All computer systems and

communication networks came to a halt. The hospital had to shut down all IT systems and revert to paper and pen based operations. This resulted in a 75% decline in daily outpatient volume and a 70% decline in daily new patient visits within the first day of the attack. Luckily, backups and system images were not affected. But the IT unit of the hospital estimated at least three weeks to rebuild the infected systems from the backups and the images. Caregivers would not be able to access any IT applications during the rebuilding process. Considering the potential negative impact on patient safety, the TMT and the BoD scrambled to have an emergency discussion at the end of the first day of the ransomware attack. They decided to authorize the payment of the ransom. Within 30 minutes of the ransom payment, hackers decrypted the systems and caregivers were able to gain access again and resume care services. To the best of the caregivers' knowledge, the one-day disruption caused by the ransomware attack did not cause any harms to patients. After overcoming the initial shock, HealthCo had yet to digest the implications of this cybersecurity breach.

PRIVACY RISKS

Identity and access management problems were also increasing privacy breach risks of HealthCo. In one incident, a secretary of a hospital executive violated privacy of PHI by viewing medical records of 750 patients from the emergency department, outside the scope of her job duties. The types of PHI she viewed included patients' names and clinical information. It was not clear how and why the secretary of a hospital executive had access to patient IT systems containing PHI.

In addition to struggling to manage identity and access rights of its own employees, HealthCo has been struggling to manage the access rights of contractor workers. Contractor wages constitute one of the highest expense items of HealthCo. After hiring them, if HealthCo cannot provide contractors timely access to the relevant IT systems, contractors remain idle and their hours are wasted. To avoid the waste, HealthCo often errs on the side of overprovisioning accounts and access rights to contractors. But the excessive access rights create privacy risks. For instance, an employee of a contractor exploited the excessive access rights to access patients' PHI without cause and e-mailed some of the PHI to his personal, unsecured e-mail account. Names, Social Security numbers, medical histories, medical insurance details, religious preferences, and other personal information of patents were exposed. The contractor disciplined the employee, but it was too late, as the privacy violation had already caused damage to HealthCo. Some patients whose data were inappropriately accessed subsequently became victims of medical identity theft. They filed a lawsuit against HealthCo for failing to protect their health information and causing harm to them through medical identity theft. HealthCo was also under investigation by the Health and Human Services due to such privacy violations.

REGULATORY COMPLIANCE

Identity and access management problems have contributed to HealthCo's rising risks and costs related to compliance with relevant laws, regulations, and industry standards. Some of the IAM related control deficiency findings were: accumulation of excessive access rights, segregation of duty (SoD) conflicts, orphan accounts, and failure to revoke access rights of terminated employees. As employees moved from role to role, or unit to unit, HealthCo kept giving them additional access rights without removing their previous access rights. After a while, employees accumulated excessive access rights, including access to conflicting roles. Deficiencies in SoD controls increased fraud risks. For instance, an accounts receivable clerk was transferred to an accounts payable clerk role, but his access from the previous role was not revoked. Having simultaneous access to accounts receivable and accounts payable roles

enabled the clerk to create fake supplier accounts and pay them, resulting in fraudulent transactions and payments.

External auditors also found many orphaned accounts because HealthCo failed to remove the accounts of terminated employees in a timely manner. Not revoking access rights of terminated employees also led to fraud. For instance, a former nurse, who became disgruntled after being terminated, collaborated with an identity theft ring. She used her unterminated account to access patient data and pass it on to the crime ring, which exploited the patient data for medical identity theft.

CYBERINSURANCE - THE WILD WEST OF INSURANCE RISKS

HealthCo would like to use cyber insurance as a risk transfer mechanism. However, it has not been easy for HealthCo to find affordable cyber insurance with sufficient coverage. Cyber is known as the wild west of insurance risks. Insurance firms face challenges in estimating and pricing cyber risks of organizations. Their cyber insurance loss ratios (claims paid/premiums collected) varied widely; some had loss ratios of over 100% suggesting losses from the cyber insurance business.

A wide variety of factors can factor into the pricing of an organization's cyber insurance premiums: e.g., type of business, industry, revenue volume, number of employees, type and scope of PII and PHI held, total number of records, maturity level of organization's cybersecurity risk mitigation mechanisms, cyber incidents experienced and cyber insurance claims filed in the past; etc. HealthCo has not ranked favorably in any of these criteria. Moreover, ransomware attacks and patient data breaches have been on the rise in the hospital industry and costs associated with a healthcare data breach were among the highest across all industries. Thus, many insurance firms are either unwilling to offer cyber insurance or demand high premiums for HealthCo's high cyber risks. Underwriters increased cyber insurance premiums of healthcare clients by 34% in 2021 and 15% in 2022.

For 2023, several insurance companies advised a coverage limit of $40Million to $50Million to be shared by 8 to 10 carriers, and quoted annual premiums ranging from $Million to $5Million. HealthCo purchased the cyber liability insurance policy that offered $50Million coverage for an annual premium of $5Million for all of its hospitals. Over the next five years, cyber insurance premiums in the hospital industry were expected to grow at an average of 15% annually. But HealthCo's insurance firm required HealthCo to meet some cybersecurity protection standards to be eligible for the renewal of its cyber insurance policy. An investment into a robust, enterprise-grade IAM across the enterprise could enable HealthCo to meet the expectations. The insurance firm was also willing to offer discounts to HealthCo for more mature cybersecurity mitigation mechanisms. A robust, enterprise-grade IAM was an essential component of a mature cybersecurity program. HealthCo's insurance firm was willing to offer a 15% discount on annual cyber insurance premiums if HealthCo adopted the on-prem version of a robust, enterprise-grade IAM solution and a 20% discount if HealthCo adopted the SaaS version. The discount on the SaaS version was higher because Cloud vendors usually have dedicated security teams and much higher level of maturity in cyberattack prevention, detection, response, and recovery compared to client companies.

THE PROPOSED SOLUTION

To address the various problems created by the IT silos across member hospitals, HealthCo had hired an IT consultancy five years ago. The consultants had recommended two workaround solutions: (1) build an enterprise-wide data warehouse to govern all patient data of HealthCo hospitals from a central location; and (2) invest in a robust, enterprise-

grade IAM application suite, such as the one offered by SailPoint, a leading IAM vendor based in Austin Texas.

HealthCo already implemented the first recommendation. While HealthCo was not yet able to standardize and integrate IT applications of its member hospitals, it was able to build a common, enterprise-wide data warehouse for housing all patient data across all member hospitals. But it was not easy to convince member hospitals and other health entities of HealthCo to put their patient data into the centralized repository. At this time, HealthCo was able to centralize about 3.2Million of an estimated total of 16million patient records across the enterprise. HealthCo aimed to double the size of this centralized repository over the next five years.

The centralization of 3.2Million patient data in a common data warehouse started enhancing patient referrals and collaborative care services across the member hospitals of HealthCo. However, the centralized repository also created a single point of failure from a cybersecurity perspective. In the past, when a member hospital was hacked, the damage was confined to the member hospital's own patient data as there was no integration among the hospitals. Now, the common data warehouse created connections and dependencies among the member hospitals of HealthCo. A data warehouse housing 3.2Million patient records was a high value target for hackers. If hackers could breach the data warehouse, they could gain access to all patient records housed there. Thus, it became critically important for HealthCo to harden the security protections of this single point of failure. The proposed IAM investment could harden the security of the data warehouse by enabling HealthCo to secure all connections to the data warehouse and systematically governing the access rights of member hospitals, caregivers, staff, and any third-party collaborators.

FUNDING OF INVESTMENT PROPOSALS

HealthCo has had many problems in using its scarce investment budget responsibly to deliver the highest business value. HealthCo's limited investment budget is not sufficient to fund all investment proposals. Deciding which proposals to fund has been problematic because different organizational units of HealthCo used different metrics to justify their investment proposals. Some units used "revenue growth" as a key valuation metric, and argued that their investment proposals would boost the revenues of HealthCo by fostering innovative new care delivery services, and attracting new patients. Some units preferred to use "cost" as a key valuation metric, and argued that their investment proposals would reduce the costs of care at HealthCo by providing efficiency and productivity gains. Some units preferred to use "risk" as a key valuation metric, and argued that their investment proposals would reduce the risks of HealthCo. Even though HealthCo's mission is to deliver high quality of care and improve patient outcomes, champions of investment proposals rarely estimate how their investment proposals would affect the quality of care and patient outcomes at HealthCo.

Due to different organizational units' use of different valuation metrics, it was infeasible to do apples-to-apples comparisons of the investment proposals coming from different units. Thus, it was not clear if HealthCo was funding investment proposals that would deliver the highest business value to HealthCo. In addition, the various metrics used in different units often interacted with each other and entailed tradeoffs. Absent an analytical framework that used a common valuation metric for the comparisons, it was not feasible to see which investment proposals would make the tradeoffs better and add the highest business value to HealthCo.

To tame some of these challenges, the CFO instituted the following funding policy. In applying for funding, champions of an investment should prepare a business case, which justifies, both quantitatively and qualitatively, how the investment would add business value to HealthCo.

- The quantitative component of the business case should estimate an investment's Total Cost of Ownership (TCO), Return on Investment (ROI), and Net Present Value (NPV). If alternative investment options are being considered, these metrics need to be used to compare them and deliver the highest value to shareholders of HealthCo.

- The qualitative component of the business case should make qualitative arguments as to how and why the proposed investment would enable HealthCo to add social and public value. Beyond the shareholders, HealthCo has many stakeholders such as patients, caregivers, the public, and regulators, who value HealthCo's contributions to patient outcomes. The Chief Medical Officer (CMO) has been refusing to consider any investment proposals that do not justify how and why they would affect access to care, quality of care, patient safety, and patient outcomes. Although the CMO's requirement has received some push-back from the proponents of technology investments, the CMO has not budged. The CMO acknowledges that it is difficult to quantify the effects of technology investments on social and public value metrics, but argues that as an organization whose mission is to deliver social and public value, HealthCo should evaluate how well a technology investment proposal would improve access to care, quality of care, patient safety, and patient outcomes, in addition to financial metrics such as TCO, ROI, and NPV.

- Any investment proposal whose 5-year TCO is in $1Million to $5Million has to be reviewed by a managerial committee made up of the Chief Executive Officer, Chief Financial Officer, Chief Medical Officer, Chief Information Officer, and Chief Compliance Officer. Any investment proposal whose 5-year TCO exceeds $5 million also requires approval from HealthCo's board of directors.

- Investment proposals that have very strong quantitative and qualitative justifications are more likely to be funded. Investment proposals whose quantified metrics are weak have lower chance of being funded, but very strong qualitative arguments might keep them in the consideration set.

Suppose, you are a team of internal champions advocating an IAM investment at HealthCo. You are asked to evaluate and recommend one of the three IAM options on the table:

(1) Do nothing: Maintain HealthCo's current legacy IAM solution;
(2) Invest in SailPoint's on-prem IAM solution;
(3) Invest in SailPoint's cloud-based, IAM software as a service (IAM-SaaS) solution.

HealthCo invited SailPoint to analyze its environment and collect some foundational data needed for the quantification of business value metrics such as TCO, ROI, and NPV. SailPoint analysts collected data about HealthCo's legacy IAM processes, tools, resources, and infrastructure. They shared their estimations about how much SailPoint IAM solutions would cost, and what kinds of benefits they would deliver to HealthCo. They summarized their methodology and raw data in an Excel Workbook which is made available to you, along with this case.

SailPoint listed the following challenges, risks and costs for HealthCo's legacy IAM:

- Challenging to protect confidentiality and privacy of patient data.
- Costly, inefficient, complex manual processes for managing identity and access of caregivers
- Error prone manual processes
- Time consuming, labor-intensive, costly regulatory campaigns to ensure compliance with regulations and requirements in a highly competitive industry
- Effort and cost intensive audit preparation, reporting, and finding remediation
- Lack of transparency and oversight of who has access to what
- Increased exposure to fraud
- Inability to cope with demand for IAM services despite a large army of people dedicated to IAM tasks.

Expectations from a robust, enterprise-grade IAM solution were:

- Automate and streamline the manual onboarding and off-boarding processes
- Reduce expensive calls to the Help Desk and replace inefficient processes
- Reduce operating costs
- Increase user productivity
- Release users' time for more productive uses
- Improve user satisfaction
- Reduce cybersecurity and privacy breach risks and costs
- Reduce fraud
- Simplify compliance preparation and reduce costs of compliance
- Enable organization to scale up IAM services without having to increase IAM headcount.
- Reduce manual labor tied up with IAM related tasks.

SailPoint's IAM solution promises to meet these expectations. SailPoint analysts summarized the modules and functionalities of the IAM solutions as follows.

IAM'S SINGLE SIGN ON MODULE

Single sign on (SSO) module enables a user to use a single ID and password, to log in to all applications they have access to, without having to use different usernames and passwords for different applications. The SSO module aims to significantly reduce the total application login time it takes per employee per day. See the SSO tab of the Excel Workbook.

Lack of an SSO module could also increase cybersecurity and privacy risks and costs. Users cannot easily remember different usernames and passwords for different applications. They often reuse the same login credential for different applications. If hackers manage to breach one application, they try the same login credential in other applications as well. Reuse of the same login credentials in multiple applications can increase the scope and damages of a breach. In the absence of a SSO functionality, users can also resort to managing multiple usernames and passwords by writing them down in unprotected digital files or sheets of paper kept in their office desks, drawers, or even next to their computer screens and keyboards. These behaviors could be easily exploited by malicious insiders or outsiders to breach confidentiality and privacy of sensitive data.

While SailPoint itself no longer offers an SSO module, SailPoint's implementation partners often source the SSO module from other IAM vendors such as Okta so the clients can assume that the SailPoint solutions are inclusive of the SSP module. The SSO module promises to improve user productivity by enabling users' single sign-on to multiple applications; increase productivity and reduce IT help desk calls by eliminating the need for

users to remember and enter multiple usernames and passwords; strengthen security by eliminating passwords when possible; and protect sensitive applications with step-up authentication based on user or access risk.

IAM'S ACCESS REQUESTS MODULE

Access request refers to an administrator's request for defining access rights and privileges of users in IT systems. New employees who join HealthCo need access to IT systems (Joiner requests). Existing employees who move from one unit/role to another, need to change access rights (Mover requests). Employees who leave HealthCo need to terminate their accounts and access rights (Leaver requests).

HealthCo frequently hires temporary nurses and other contract workers. It needs to provision access to them for some IT applications for a temporary period of time, and terminate their access when the assignment period is over. HealthCo also often rotates caregivers across units. It needs to revoke their access rights from the old unit's applications and grant them access to applications of the new unit. When caregivers of one unit are called to another unit to collaborate on patient care on an emergency basis, HealthCo needs to provision temporary access to them to the applications at the destination unit, and revoke the access when the emergency collaboration is over.

HealthCo's legacy IAM has manual processes for enabling the review and approval of such access requests. Manual processes are error-prone, inconvenient, take excessive amounts of time and causes delays in operations, and reduce labor productivity and user satisfaction. When HealthCo cannot provide access to caregivers in a timely manner, care services could be disrupted or delayed. When HealthCo cannot revoke access rights of terminated employees in a timely manner, fraud, cybersecurity and privacy risks go up. In the past, some terminated employees became disgruntled and tried to gain unauthorized access and copy sensitive patient data weeks after their termination because HealthCo was not able to revoke their access rights in a timely manner. HealthCo has also failed to revoke the old access rights of employees in a timely manner when they moved from one unit to another, or they became promoted to new roles. As a result, employees have accumulated too much access rights. In the past, external auditors caught such problems and wrote up HealthCo for deficiencies in segregation of duty (SoD) controls. The auditors alerted management of HealthCo that SoD control deficiencies create opportunities for fraud, and cybersecurity, and privacy breaches. With manual access request processes, HealthCo has struggled to remediate such audit findings in a timely manner. It has also incurred significant costs to remediate the audit findings.

SailPoint argues that its Access Request Module could address many of these issues by automating some of the manual access request processes and providing administrators with more productive means of making and servicing the access requests. SailPoint analysts collected some data on access request patterns in HealthCo for use in the quantification of the benefits of the access request module. See the Access requests tab of the Excel Workbook.

IAM'S PROVISIONING MODULE

Provisioning is a business process for setting up user accounts for access to HealthCo's networks and enterprise resource planning (ERP) application suite. Provisioning volumes are high at HealthCo due to frequent use of mergers, acquisitions, divestitures, internal restructurings, outsourcing and other third party contract work. When HealthCo acquires another healthcare organization, it has to onboard the acquired organization's employees to

some of its own IT systems and provision network and ERP accounts to them. When HealthCo divests an existing unit, it has to de-provision network and ERP accounts of the divested unit's employees in a timely manner. When HealthCo goes through organizational restructuring, changes in employee units/roles require account provisioning/de-provisioning. When HealthCo outsources some systems and processes or hires contractors to do the work on its premises, it also needs to provision network and ERP accounts to them.

Currently, HealthCo has manual provisioning processes which use paperwork trail and approval signatures from various administrators. Creating, reviewing, approving, and routing the provisioning requests take a long time. The delays incurred also cause disruptions in care delivery processes and could negatively affect patient outcomes. Delays and errors in provisioning/de-provisioning processes could also increase HealthCo's fraud, cybersecurity, privacy, and compliance risks and costs.

SailPoint analysts claim that the provisioning module of their IAM solution can reduce the times, costs, and risks entailed. The provisioning module could reduce the wait times by fully or partially automating and optimizing the provisioning/de-provisioning workflows. It could potentially improve end user productivity through fast, automated processing of account requests and reduce administrative burden on IT and help desk personnel. It can enable HealthCo to implement automated protection and detection controls over the provisioning processes to reduce errors, mistakes, and accordingly fraud, cybersecurity, and privacy risks. Provisioning accounts in a controlled manner can also enable HealthCo to meet the requirements of regulatory compliance audits faster and at lower cost. If there are any audit findings, remediating them would be easier due to the automated capabilities for provisioning accounts. SailPoint analysts collected some data on the number of provisioning requests and the time it takes to address them. Please see the Provisioning tab of the Excel sheet.

IAM'S PASSWORD MANAGEMENT MODULE

Currently, due to the decentralized governance of IT across organizational units, there is no capability to manage passwords in a unified way. Users have to maintain different passwords for different IT systems and applications they need to access. This creates many password management problems. Users often forget their passwords. In trying different passwords and failing to get it right, they have their accounts locked. There is no self-service capability to allow users to reset their passwords and unlock accounts on their own. Users have to contact the IT help desk to have an IT staff to reset the password and unlock the account manually. This process consumes a lot of time and reduces productivity of both the user and the IT staff. The manual password management processes also make the IT staff more vulnerable to social engineering attacks: malicious users try to gain access to systems by impostering as HealthCo employees needing to reset their passwords.

SailPoint claims that the password management module of its IAM solution could at least partially automate the password management processes to provide self-service capabilities and reduce the time, costs, and risks entailed in manual password reset and account unlock requests. The password management module also allows HealthCo to implement an enterprise-wide password policy and enforce more complex password requirements. In the Password Management tab of the Excel Workbook, SailPoint analysts present data on password reset request volumes and times at HealthCo and how SailPoint's password management module could improve them.

IAM'S CERTIFICATIONS MODULE

Certification campaigns are used to have managers review and certify their subordinates' roles, access profiles, entitlements, apps, etc. in IT systems of a firm. Systems administrators periodically run certification campaigns and ask managers to review and approve their subordinates' access rights and privileges. Administrators typically create certification campaigns for all "reviewers" in an organization. Reviewers are business managers who are responsible for the users. When an administrator creates a certification campaign that contains access items or users that a business manager is responsible for, the manager receives a notification that certifications are ready for her review. A list of identities that are included in the certification is displayed. For each identity, the manager sees the following:

- **Exceptions**. This is a count of any access items that are either new or marked as privileged. (The first time the company runs certifications, all access items are considered new).
- **Reassigned**. If the employee was reassigned to a manager from someone else, an information icon is shown here so that the manager can click on it to see why it was reassigned.
- **Decisions left**. This indicates how many access items still need to be reviewed by the manager.
- **Status**. This indicates whether the certification has been completed for that person.

The certifications module of the IAM solution aims to reduce the firm's cost of compliance by automating labor-intensive access review processes. It also seeks to strengthen controls to address audit deficiencies or weaknesses; provide proof of compliance to internal and external auditors; and mitigate risks through proactive detection and prevention of inappropriate access and violation of corporate policies. See the Certification Campaigns tab of the Excel Workbook for the data collected by SailPoint analysts on the number of certification campaigns at HealthCo, the average time they take, and how SailPoint's module might improve them.

IAM'S AUDITS MODULE – Remediation of Audit Findings

SailPoint's Audits Module aims to increase clients' ability to comply with laws, regulations, and industry standards; and reduce the costs of compliance and remediation efforts. Healthcare is a highly regulated industry. Complying with regulations such as HIPAA and HITECH, and meeting requirements such as meaningful use have proved challenging and costly.

SailPoint's Audits Module implements compliance controls to streamline audits and finding remediation processes. With a centralized identity database, defined workflows, and automated processes, HealthCo can expect fewer instances of practices running counter to security and access policies evaluated in the audits. Thus, the Audits Module can reduce the number of audit findings. It can also reduce the costs associated with the remediation of the audit findings. Audits tab of the Excel Workbook lists some data collected by SailPoint analysts on audits, findings, remediation costs in HealthCo and how the Audits Module can improve them.

RETIREMENT OF HEALTHCO's LEGACY IAM SOLUTION

HealthCo has an in-house developed, legacy IAM system. It has many weaknesses such as not fully automating the various IAM processes summarized above; not having a modular

design architecture; requiring a dedicated IT infrastructure and support team; and not having state-of-the-art IAM expertise in the team. As HealthCo's IAM needs evolve and change over time, the dedicated support team for the legacy IAM has to undertake in-house development projects to add new functionality or upgrade the existing functionality of the legacy IAM. The team is often overwhelmed with day-to-day run time related challenges and does not have the bandwidth or talent to add innovative new functionality requested by user organizations. The legacy IAM meets the minimum required IAM needs of HealthCo, but it is not able to catch up to the standards of modern IAM systems offered by IAM vendors. The costs associated with the legacy IAM solution are listed in the Legacy IAM tab of the Excel Workbook. SailPoint's IAM solution seeks to rip and replace the legacy IAM solution of HealthCo.

SailPoint consultants estimate that they would need about six months to ingest HealthCo's IAM data to build identity cubes and another six months for setting up the new hardware and software infrastructure, testing them, training users, and making SailPoint's IAM solution functional. Thus, after HealthCo makes the decision to invest in SailPoint's IAM, it would take about a year to switch from legacy IAM to SailPoint's IAM and start seeing the promised benefits.

SAILPOINT'S IAM SOLUTIONS

SailPoint offers an On-Prem version and a SaaS (cloud) version of its IAM solution. The On-Prem version is a set of IAM software modules that are sold to clients based on a licensing fee payment model. The client installs and runs the on-prem version on its own IT infrastructure. This gives the client full control over, as well as the responsibility, for operating and securing the on-prem IAM version. During the initial set-up, SailPoint can provide support to clients for an initial set-up fee. When SailPoint releases new version of the on-prem IAM software suit, clients need to pay for upgrading to the new version. The Excel Workbook tab entitled, "11.CostsOfSailPoint-On-Prem-IAM," lists the costs SilPoint identified for adopting and running the on-prem version of SailPoint's IAM. HealthCo may need to do additional research to assess if there might be any intangible, hidden costs of the on-prem version, not listed by SailPoint.

The SaaS version of IAM is offered to clients from SailPoint's Cloud Infrastructure. SailPoint is responsible for installing, operating, and upgrading the IAM-SaaS version on its own Cloud infrastructure. Application access requests initiated by client firms' computers go through the Internet to SailPoint Cloud, approved or denied, and come back to the client computers. Thus, it is critical to for all HealthCo units to have reliable and secure Internet connections to ensure that the IAM transactions taking place over the Internet through SailPoint's SaaS are also reliable and secure. To connect clients' computers to SailPoint's IAM-SaaS version, there is a one-time set-up. SailPoint helps with the set-up for a fee. SailPoint analyzed summarized the costs associated with the SaaS version in the Excel tab entitled, "10. CostsOfSailPoint-SaaS-IAM." HealthCo employees have heard that SaaS vendors only show the tangible costs visible in the "tip of the cost iceberg" when listing SaaS costs. They may have to do additional research to identify cost items buried below the surface, at the bottom of the cost iceberg.

For instance, when switching to SaaS, the reliability and security of the client's Internet connections are the responsibility of the client. Most of HealthCo's hospitals are located in rural areas. Although Internet is available in the rural areas, bandwidth and reliability are often problematic. HealthCo may need to renew its contracts with Internet Service Providers to request higher quality of service guarantees. Such items are additional costs not covered in SailPoint's list.

SailPoint charges an annual subscription fee per user of the Saas-IAM. HealthCo employees about 125,000 full time employees and 2500 full time equivalent (FTE) contractors. As stated in the "2. Miscellaneous data" tab of the Excel Workbook, HealthCo estimates that only about 55% of its employees and contractors would need SaaS subscriptions.

MISCELLANEOUS DATA

SailPoint summarized various other parameter values about HealthCo in the "Miscellaneous data" tab of the Excel Workbook: e.g., revenues, IT budget, employee roles and salaries, contractors, labor and salary growth rates, workdays, discount rate, bank loan rate, percent of employees and contractors who need to use IAM per year, annual cyber insurance premiums of HealthCo with legacy IAM, cyber insurance discount rates if HealthCo were to adopt a modern IAM, etc.

CYBER LOSS EXPOSURE

SailPoint and other industry experts argue that investing in a robust IAM solution would reduce HealthCo's likelihood and impact of cybersecurity and privacy breaches. As a result, the IAM investment can change HealthCo's Cyber Loss Exposure (CLE). The standard Excel Workbook prepared by SailPoint did not contain a tab for the CLE estimates. But HealthCo employees followed the guidance provided by the FAIR Institute to put together some data for estimating the CLE metrics for the three IAM options on the table. Please see the Excel tab titled, "12. Risk-CyberLossExposure(CLE)."

Group Assignment: All HealthCo assignments are group assignments. Peer evaluations will be done at the conclusion of the HealthCo assignments on 12/4. Peers will assess relative contributions of group members to group deliverables.

HEALTHCO PART – I: TCO (3% of final grade)
(Due by 6:00am on November 8, 2023)

Total Cost of Ownership (TCO)

a. Estimate the TCO for all three IAM options on the table for the 5-year period:
    i. TCO of keeping the legacy IAM of HealthCo
    ii. TCO of investing in SailPoint-IAM-On-Prem version
    iii. TCO of investing in SailPoint-IAM-SaaS version

    Show the details of your TCO computations in the relevant tabs of the HealthCo Excel Workbook.

    If the data in the Excel Workbook or the case are not sufficient to do the TCO estimations (e.g., any major intangible costs not mentioned by the vendor), you can do independent research to find the additional data you need or make assumptions about the uncertain parameters. If you make assumptions, explicitly state them and justify why they are plausible assumptions.

b. If HealthCo were to make a selection based on the TCO metric alone, which of the three IAM options would you recommend?

DELIVERABLES OF PART I:

- **HealthCo Excel Workbok** containing your supporting computations for TCO. Make sure that your Excel computations are organized well enough to be understood easily by the decision makers (e.g., clearly label all the variables, equations, and explicate and justify any assumptions made, etc.).

- **A PPT slide deck** for doing a 10-minute presentation of your recommendation and supporting evidence (cover a, b). Your goal is to convenience the decision makers to support your recommendation. Be prepared to do this presentation in class.

- **Deadline:** Please upload your deliverables to Canvas by the 6:00am deadline on the due date (preferably much earlier). This is important because Teaching team will prepare a table summarizing all group's results before the class start time. Any submissions that miss the 6:00am deadline will incur a late submission penalty of 10pts.

During the session, we will randomly select a few groups to present their findings. We will also ask the remaining groups to compare their findings with those of the presenting groups.

HEALTHCO PART – II: ROI and NPV (6% of final grade)
(Due by 6:00am on November 13, 2023)

Return on investment (ROI):

a. Estimate the ROI values of HealthCo's potential investments in SailPoint's two IAM versions for the 5-year period:
    i. SailPoint's IAM-On-Prem version

ii. SailPoint's IAM-SaaS version

Compute the ROI of an IAM investment using the following equation:
ROI= (Total Cash Inflows - Total Cash Outflows / Total Cash Outflows).
Calculate "Total Cash Inflows" from an IAM investment over the 5-year period by estimating the productivity savings to be provided by the IAM investment.

Calculate "Total Cash Outflows" associated with an IAM investment over the 5-year period by estimating the cash payments to the IAM vendor for cost items such as the initial set-up service costs, licensing fees of IAM software modules for the on-prem version or per user subscription fee for the SaaS version, etc.

Show the details of your ROI computations in the Excel Workbook.

If the data in the Excel Workbook or the case are not sufficient to do the ROI estimations, you can do research to find the additional data you need or make assumptions about the uncertain parameters. If you make assumptions, explicitly state them and justify why they are plausible assumptions.

b. If HealthCo were to make a decision based on the ROI metric alone, which of the three IAM options would you recommend?

Net Present Value (NPV):

c. Estimate the Shareholder Wealth effects of the investments in SailPoint's two IAM versions for the 5-year period:
   i. NPV for SailPoint's IAM-On-Prem version
   ii. NPV for SailPoint's IAM-SaaS version

   For purposes of this assignment, assume that Shareholder Wealth = Net Present Value (NPV) of net cash flows from an IAM investment.

   Compute the net cash flows from an IAM investment in each year during the 5-year period; use HealthCo's discount rate in discounting the net cash flows to the present year, to obtain the NPV of the net cash flows from the investment.

   Show the details of your NPV computations in the Excel Workbook.

   If the data in the Excel Workbook or the case are not sufficient to do the NPV estimations, you can do research to find the additional data you need or make assumptions about the uncertain parameters. If you make assumptions, explicitly state them and justify why they are plausible assumptions.

d. If HealthCo were to make a decision based on the NPV metric alone, which of the three IAM options would you recommend?
e. Considering all three metrics you estimated so far, TCO, ROI, and NPV, which of the three IAM options would you recommend; and why?

DELIVERABLES OF PART II:

- **HealthCo Excel Workbok** containing your supporting computations for ROI and NPV. Make sure that your Excel computations are organized well enough to be understood easily by the decision makers (e.g., clearly label all the variables, equations, and explicate and justify any assumptions made, etc.).

- **A PPT slide deck** for doing a 10-minute presentation of your recommendations and supporting evidence (cover a, b, c, d). Your goal is to convenience the decision makers to support your recommendation. Be prepared to do this presentation in class.

- **Deadline:** Please upload your deliverables to Canvas by the 6:00am deadline on the due date (preferably much earlier). This is important because Teaching team will prepare a table summarizing all group's results before the class start time. Any submissions that miss the 6:00am deadline will incur a late submission penalty of 10pts.

During the session, we will randomly select a few groups to present their findings. We will also ask the remaining groups to compare their findings with those of the presenting groups.

HEALTHCO ASSIGNMENT PART – III: CLE (3% of final grade)
(Due by 6:00am on November 15, 2023)

a. Estimate HealthCo's annual Cyber Loss Exposure (CLE) using the data provided in the case and the tab entitled "12. Risk-CyberLossExposure(CLE)" in HealthCo's Excel Workbook. In the same tab, show your estimations of CLEs for all three options:
   - With legacy IAM
   - With On-Prem version of SailPoint's IAM
   - With SaaS version of SailPoint's IAM

b. If HealthCo were to make a decision based on the CLE metric alone, which option would you recommend?

c. Now consider not just the CLE metric but also the TCO, ROI, and NPV metrics you estimated earlier. Based on the four metrics, which IAM option would you recommend to HealthCo and why?

DELIVERABLES OF PART III:

- **HealthCo Excel Workbok** containing your supporting computations for CLE. Make sure that your Excel computations are organized well enough to be understood easily by the decision makers (e.g., clearly label all the variables, equations, and explicate and justify any assumptions made, etc.).

- **A PPT slide deck** for doing a 10-minute presentation of your recommendations and supporting evidence (cover a, b, c). Your goal is to convenience the decision makers to support your recommendation. Be prepared to do this presentation in class.

- **Deadline:** Please upload your deliverables to Canvas by the 6:00am deadline on the due date (preferably much earlier). This is important because Teaching team will prepare a table summarizing all group's results before the class start time. Any submissions that miss the 6:00am deadline will incur a late submission penalty of 10pts.

During the session, we will randomly select a few groups to present their findings. We will also ask the remaining groups to compare their findings with those of the presenting groups.

SESSION-26 (11/27): ZOOM TUTORIAL ON @RISK TOOLS

This is a Zoom-only session: https://utexas.zoom.us/j/94895611128
The goal is to introduce you to @RISK tools that you will need to prepare Part IV of the HealthCo assignment. Come to the session with @RISK installed on your computer.

- Conducting sensitivity analysis with Monte Carlo simulations
- Download and install @RISK tools of Palisade (now Lumivero)
- @RISK Guided Tour - Basic Features - Sensitivity Analysis https://www.youtube.com/watch?v=TT10GJ0nTKE
- Learn basic functionality of @RISK: https://www.palisade.com/videos/
- For additional guidance and tutorials on @RISK tools, see YouTube channel of @RISK: https://www.youtube.com/@RISKbyLumivero/videos

SESSION-27 (11/29): ZOOM TUTORIAL ON FAIR-U

This is a Zoom-only session: https://utexas.zoom.us/j/95487312921
The goal is to introduce you to FAIR-U tool that you will need to prepare Part IV of the HealthCo assignment. Create a FAIR-U account before coming to this session and do the assigned readings:

- Sign up for a free FAIR-U account (https://www.fairinstitute.org/fair-u), do the sample exercise in preparation for applying this risk quantification tool to HealthCo case.
- Estimating cyber loss exposure
- **(Canvas)** Jones, J. (2023). "Today's Cyber Risk Measurement Best Practices." FAIR Institute.
- **(Canvas)** Martin-Vegue, T. (2021). "The Elephant in the Risk Governance Room." ISACA.

HEALTHCO ASSIGNMENT PART – IV: Sensitivity Analysis and Loss Exceedance Curve (8% of final grade)
(Due by 6:00am on December 4, 2023)

SENSITIVITY ANALYSIS:
After seeing your preliminary analyses in #I through #III above, the CFO challenged many of the static parameter values you used in your estimations. She acknowledges that the employees of HealthCo might have provided some of those static values. While she is confident about values of some parameters, she informs you that there is significant uncertainty around some other parameter values. Instead of using fixed values for the uncertain parameters, she wants you to a range of values and do sensitivity analyses: how would the outcomes of interest change as the values of uncertain parameters change? The CFO asks you to focus on the NPV outcome per se. In the following table, she provided the distributions of several uncertain parameters. She expects you to run Monte Carlo simulations, using the @RISK add-in of Excel, to assess the sensitivity of NPV outcomes to uncertain parameters.

Uncertain parameters	Distribution	Mean (μ)	Std. Dev. (σ)
% of HealthCo employees & contractors who use IAM/year	Normal	55%	19%
Annual growth rate of IT applications at HealthCo	Normal	7%	3%
Target productivity improvement rate of SailPoint's IAM (originally it was fixed at 80% in SSO, Access, Provisioning, Password, Certifications, Audits modules. Now it will vary in a range).	Normal	60%	12%

Annual growth rate of the requests or events managed by the SSO, Access, Provisioning, Password, Certifications, and Audits modules.	Normal	5%	1%
Annual growth (or shrinkage) rate of the number of employees and contractors at HealthCo	Normal	5%	10%
Annual salary hike rate of employees and contractors at HealthCo	Normal	5.5%	2.36%
Total number of patient records at risk	Normal	3,200,000	1,375,500
Annual breach probability with Legacy IAM	Pareto2	$\boldsymbol{b}$=1	$\boldsymbol{q}$=6.6
Annual breach probability with SailPoint On-prem	Pareto2	$\boldsymbol{b}$=1	$\boldsymbol{q}$=20
Annual breach probability with SailPoint SaaS	Pareto2	$\boldsymbol{b}$=1	$\boldsymbol{q}$=139
Annual growth (or reduction) rate of HealthCo's cyber insurance premium	Normal	15%	7.5%
Discount rate of HealthCo	Normal	10%	4.3%
Annual bank loan rate of HealthCo	Normal	7%	2%
Annual inflation rate in the US in the next 5 years	Normal	5%	1%

a. Run 10,000 iterations of a Monte Carlo simulation to identify which uncertain parameters listed in the table above have the highest impact on the NPV outcomes. Depict your results with Tornado graph and Spider graph tools of @RISK.
b. Explore under which value ranges of the uncertain parameters, the NPV of the On-Prem version might become greater than the NPV of the SaaS version, or vice versa.
c. Build on the insights emerging from the sensitivity analyses to make recommendations to HealthCo executives as to how they should negotiate the IAM contract with SailPoint.

Loss Exceedance Curve:

d. Use the FAIR-U tool (https://www.fairinstitute.org/fair-u) to generate "Loss Exceedance Curves" of the legacy IAM and the SailPoint's IAM solution you recommended.
e. Explain to HealthCo executives how they should interpret the loss exceedance curves in making the investment decision.

f. Reflecting on all your estimations (TCO, ROI, NPV, CLE, sensitivity analyses, Loss Exceedance Curves) and all key qualitative factors, make and justify your final recommendation to the HealthCo executives.

DELIVERABLES

- **Executive Summary**. Prepare an executive summary to HealthCo to present and support your recommendation with quantitative and qualitative arguments. Format of the Executive Summary: Word document, maximum of 5 pages (preferably shorter), single line spacing, 1" margins on all sides, Verdana font type, and 10 point font size.

- **Excel sheet** containing your supporting computations. Make sure that your Excel computations are organized well enough to be understood easily by the decision makers (e.g., clearly label all the variables, equations, and explicate and justify any assumptions made, etc.).

- **A PPT slide deck** for doing a 10-minute presentation of your recommendations and supporting evidence. Your goal is to convenience the decision makers to support your recommendation. Be prepared to do this presentation in class.

Please upload your deliverables to Canvas by the 6:00am deadline on the due date (preferably much earlier). Teaching team will try to quickly look at the results by 8am, class start time, to see how the estimations of groups vary.

During the session, we will randomly select a few groups to present their findings. We will also ask the remaining groups to compare their findings with those of the presenting groups.