Twitter’s 2020 Hack: Addressing X’s IAM Controls

BLUESTONE ADVISORS

Binyan Hu

Sourabrata Samanta

Nikhil Sista

Katia Torres Sanchez

AGENDA

- Context
- Recommendation
- Timeline
- Financials
- Risks and Mitigation
- Conclusion

The Twitter 2020 Hack exposed IAM protocols that were not aligned with best practices and the industry standards

Twitter Internal Controls

As the globally recognized social media platform, X has been widely used by individuals, politicians, celebrities, and business leaders. To maintain secure communication and protect the privacy of its users, X employs various internal tools and security protocols, aiming to deliver a safe and trustworthy environment for millions of daily users.

Twitter Hack

The Twitter 2020 hack **exposed weak access controls and over-privileged employee accounts.** Hackers exploited these weaknesses through social engineering, **revealing flaws in employee security practices**. The breach damaged X's reputation and raised potential legal concerns about data protection.

Question

How can X manage identities and access of an army of people without hiring an army of people?

We suggest X deploy a comprehensive and holistic IAM solution that meets industry standards and provides better access security

IAM

A strategic approach to managing digital identities and access rights, ensuring the right people have the right access to the right resources at the right time

Identification

Identity management

Highlights the financial and reputational risks of social engineering attacks, advocating for proactive defenses

Authentication

Multi-layered Authentication

Measures aim to protect against unauthorized access by using physical tokens, detecting unusual behaviors, and enabling real-time alerts for suspicious activity

Authorization

Persistent Access Control

Measures collectively aim to reduce unauthorized access risks, improve accountability, enhance compliance, and increase operational efficiency

External User Control

Enhancing external user control by addressing weaknesses in the current IAM architecture, to reduce security breaches, and improve the overall user experience during security incidents

X needs to improve identity management by ensuring employees are trained to recognize social engineering schemes and adhere to best practices

Social Engineering

Regular Phishing Simulations

- Conduct routine phishing simulations to help employees recognize fraudulent communications
- Scenarios must be realistic and relevant to X's operations
- Employees who succumb to phishing scams must have refresher training course to understand how to recognize social engineering scams

Mandatory Training

- Mandate security awareness training more frequently
- Stress the importance of security protocols in remote work environments
- Encourage a culture that shows employee verifying unusual requests and reporting suspicious activities immediately is the standard

Improve Internal Communications

- Use an authenticated system for internal support calls, so employees can verify that an incoming call is genuinely from the IT department

Identity Management with AWS IAM Management Service

Centralized Identity Repository	A centralized identity repository is a single source of truth for all identities within X. It will manage identity attributes, such as department and role. It will securely store verified identity data.
Identity Reauthentication	Require employees to reauthenticate through a separated, secure channel. The mode of reauthentication should not be the same as the original request.
Identity Monitoring	X must continuously monitor for unusual locations of users and the access of resources users rarely use. There should be an alert system in place to raise concerns of any identity violations.
Identity-Based Networking	X can have better control of access by verifying identities based on their location. It will enhance security while supporting the remote work environment.

Importance of Strong Identity Controls

98% of cyberattacks rely on social engineering" *-Splunk*

$130k "Average cost of a social engineering attack" *-Splunk*

-4% drop of stock shares after attack *-Reuters*

Source: Amazon

X needs to implement a multi-layered, Phishing-Resistant Authentication System to increase its overall authentication capability

Deploy Phishing-Resistant MFA	• Avoid SMS-based MFA, which is vulnerable to interception and SIM-swapping attacks • Adopt stronger MFA methods such as FIDO2 hardware tokens (e.g., YubiKey) for remote employees and biometric authentication (e.g., fingerprint or facial recognition) for mobile devices and workstation to ensure robust protection against phishing attacks	**Benefits** Enhances security by requiring either a physical token or unique biometric data, making unauthorized access significantly more difficult for attackers. Organizations that implemented FIDO2 authentication experienced up to a 99.9% reduction in successful phishing attacks	**$1.6M** Reduction in data breach cost -IBM
Integrate Continuous Behavioral Biometrics	• Incorporate continuous behavioral biometrics, such as monitoring typing patterns, mouse movements, and login times • Set up automated triggers for additional verification or temporary account suspension when anomalies or suspicious behavior are detected, enhancing real-time protection	**Benefits** Provides real-time detection of compromised accounts by identifying and flagging unusual login behaviors, offering a proactive defense layer that responds to anomalies before they lead to a security breach	**90%** Detection accuracy -Microsoft
Implement AI-Driven Phishing Detection and Alert Systems	• Use AI-based solutions to detect, flag and respond to phishing attempts in real-time • Configure the system to automatically alert both employees and the IT security team of any suspicious login attempts or abnormal MFA requests, enabling quick intervention	**Benefits** Prevents successful phishing attacks by identifying and flagging suspicious behavior early and enabling a quick response, reducing the likelihood of an attacker gaining access	**40%** Faster response to phishing -Forrester

X needs to implement persistent access controls that provide comprehensive oversight and limit potential vulnerabilities

Measures to be taken		Benefits	
Principle of Least Privilege (PoLP)	Employees only have access to the resources necessary for their job functions. This reduces the attack surface by minimizing permissions and limiting the impact of a compromised account	**Reduced Risk of Unauthorized Access**	By restricting and continuously monitoring access, the chances of successful phishing and social engineering attacks are diminished
Role-Based Access Control (RBAC)	Define and enforce role-specific access within the organization. Assign permissions based on job roles to streamline management and auditing of access rights, ensuring employees have only the access they need	**Improved Accountability and Transparency**	Detailed access audits and session logs provide clear insights into user activity, enabling organizations to trace suspicious actions back to their source
Continuous Access Monitoring and Automation	Define and enforce role-specific access within the organization. Assign permissions based on job roles to streamline management and auditing of access rights, ensuring employees have only the access they need	**Enhanced Compliance and Data Security**	Following best practices in access control aligns with data protection regulations and minimizes potential legal exposure
Just-In-Time (JIT) Access Control	Implement JIT access to grant temporary and time-limited permissions for critical systems as needed. This prevents employees from retaining unnecessary access, significantly reducing the risk of internal abuse or accidental data exposure	**Operational Efficiency Without Increased Headcount**	Automated tools and defined access protocols help manage identity and access at scale without the need for large administrative teams

We aim to protect external users by preventing risks that could lead to catastrophic consequences and negative press for X

Current State IAM Architecture		Future State IAM Architecture	
Limited user control in security emergencies Users couldn't lock accounts to stop unauthorized access, leaving high-profile accounts exposed for hours before response	How? →	**Instant Account Lockdown**	A "Lock My Account" feature freezes accounts immediately, cutting time-to-secure and giving users total control
Generic alerts that users ignore or dismiss Users dismiss frequent alerts, causing alert fatigue and nearly half of breaches to go unaddressed	How? →	**Security Smart Alerts, only when needed**	AI-driven alerts notify users only for real threats, reducing alert fatigue and boosting response rates. This can also take advantage of other forms of notification, specified by the user
Inadequate security defaults for users Less than 3% of accounts used MFA, leaving most users targets for phishing and attacks due to insufficient default protections	How? →	**Always-On Security Defaults**	Built-in protections, like MFA and link detection, slash unauthorized access attempts with seamless, automatic security
Painfully Slow Recovery Recovery times stretched to hours or days, with complex, frustrating steps that left users locked out and unsupported	How? →	**Rapid Recovery within minutes**	Multiple verification options, like biometrics, restore access faster, making account recovery smooth and frustration-free

Source: Wired

The proposed IAM project is a 1-year implementation plan divided into four phases that will run concurrently

Activities	Months											
	Aug-20	Sep-20	Oct-20	Nov-20	Dec-20	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21
Identity Management												
Phising simulations												
Social Engineering Employee Training												
Centralize Employees' Identities into a Single Repository												
Expand Identify-Based Networking capabilities to remote workers												
Access Management - Authentication and Authorization												
Update and redefine PoLP, RBAC, and JIT Access controls												
Security Assessment												
Biometric Authentication Infrastructure Setup												
Deploy Phising- Resistant MFA												
Deploy AI - Driven Phishing Detection												
Implement Continous Behavioral Biometrics												
AI Compresentive Testing												
External IAM												
Strengthen External Functions												
Ongoing												
Monitor IAM controls												

The journey to $60 million in benefits begins with a bold IAM investment, achieving a 34% ROI and reaching break-even in just 30 months, setting X up for lasting success

ROI

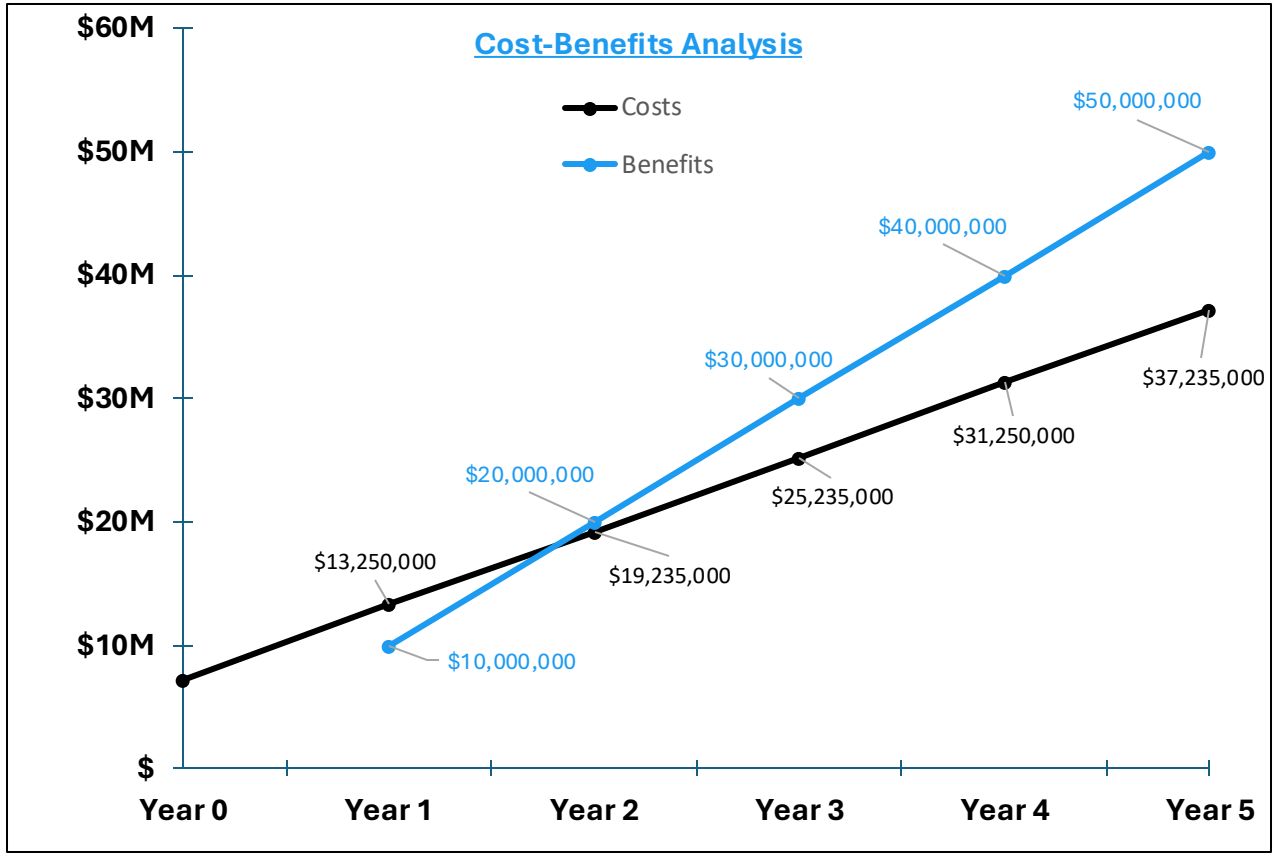
34%

B/E

~ 2 years

NPV

$9.2M



Financial Assumption

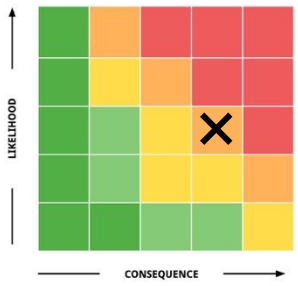
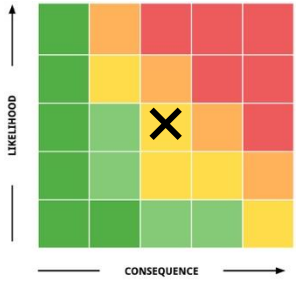
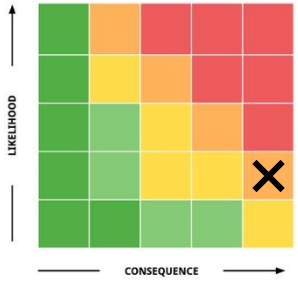
The frequency of FTC regulatory inquiries directed at X will be reduced by 20% through our solution

Total Benefits	$50M
Cost Avoidance (Fines, IAM-related system downtime, etc)	$50M

Total Costs	$37.2M
Total One-time Costs	**$1.2M**
Initial Purchase, Infra Setup, and Configuration	$350K
Phishing Detection Setup	$185K
Total Recurring Costs	**$37.2M**
IT Infrastructure Costs of supporting solution	$18M
Software & Hardware Licensing Fees	$15M
Follow-up training and support costs	$1.8M

Note: Cost values are not all inclusive, see appendix

Our proposed Identity and Access Management (IAM) enhancement has potential risks that could be mitigated with strategic planning

Potential Risk	Risk Matrix	Mitigation Plan
Social Engineering is More Sophisticated Attackers are taking advantage of AI to target employees more effectively. The phishing emails look more credible and seem to originate from an internal source. Employees might still fall victim to these scams, which can lead to data breaches or other compromises of company information.		• Constantly update the training to adhere to current technology • Simulations should change routinely and adapt to any new practices of social engineering attacks • Require employees to use an internal directory to call back a caller to verify their identity
Employee Resistance Enforcing new security measures, such as biometric authentication, may result in employee resistance. Employees may feel the requirements of facial recognition or fingerprint scans is too intrusive and violates their privacy.		• Highlight privacy protections that X is taking to safeguard employees' data • Demonstrate the benefits employees will have, such as faster logins and better security in protecting sensitive information • Implement policies that automatically delete biometric data when they leave X
Evolving Regulatory Requirements As AI continues to develop, it is important that X adapts to the changes it poses to its security measures. However, regulatory requirements are continuously changing to catch up with newer disruptive technologies. X could risk being noncompliant and face legal repercussions due to changing regulatory demands.		• Perform regular audits to ensure the new IAM practices align with regulatory requirements • Automate compliance monitoring to flag non-compliant access patterns or data handling practices

To recover from the Twitter 2020 Hack and prevent a similar attack from occurring again, X needs to enhance its Identity and Access Management

Identity Management & Training

Identity Management will help reduce the risk of sophisticated Social Engineering attacks

- Employee training
- Centralized identity repository
- Identity-based Networking

Stronger Access Management

Authentication Management will ensure the right people have access to what they need

- Multi-Factor Authentication
- Biometrics
- Controls: JIT, PoLP, RBAC
- AI and Automation

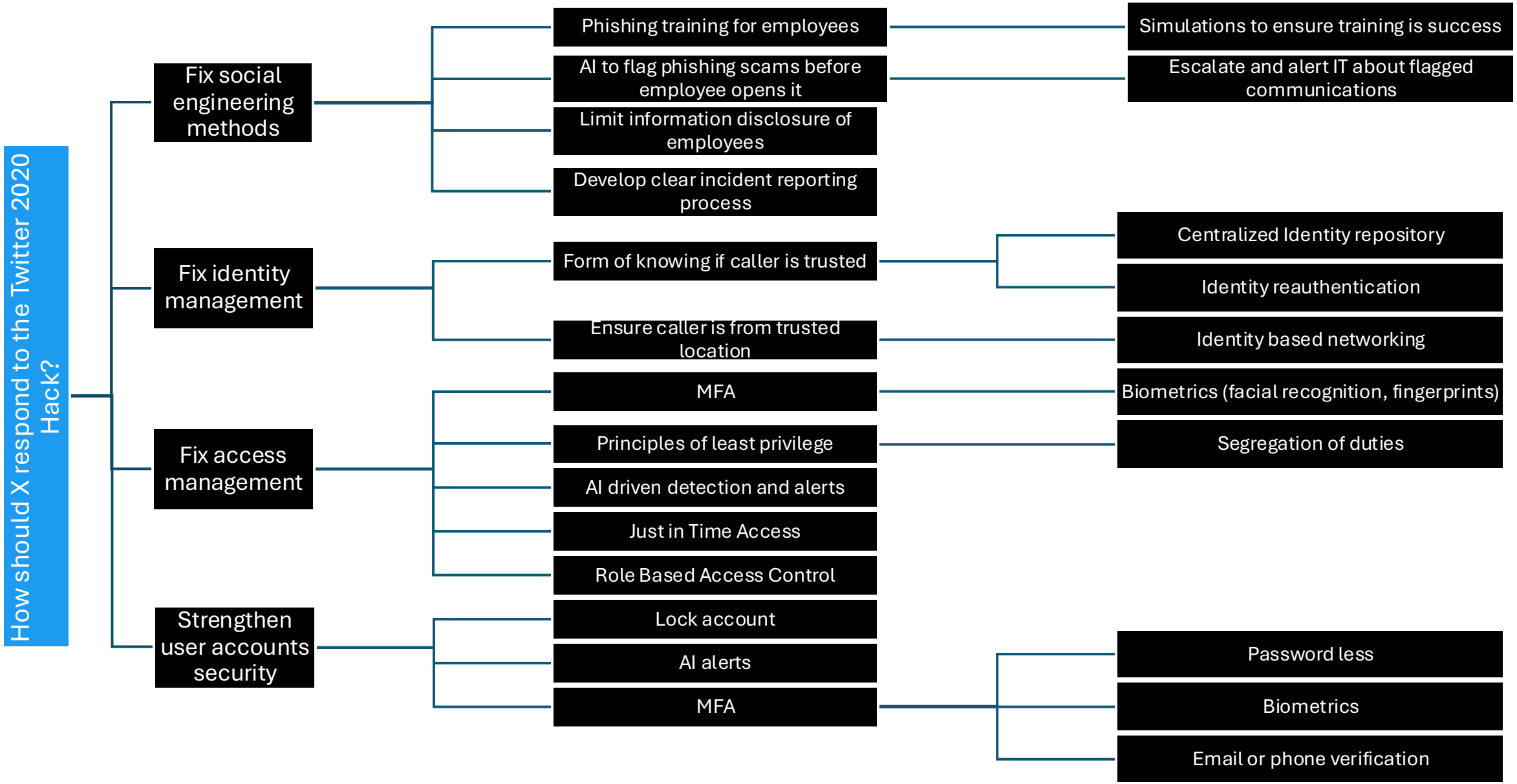
Enhanced IAM for External Users

IAM components, such as lockdown account and alerts, will prevent accounts from being compromised

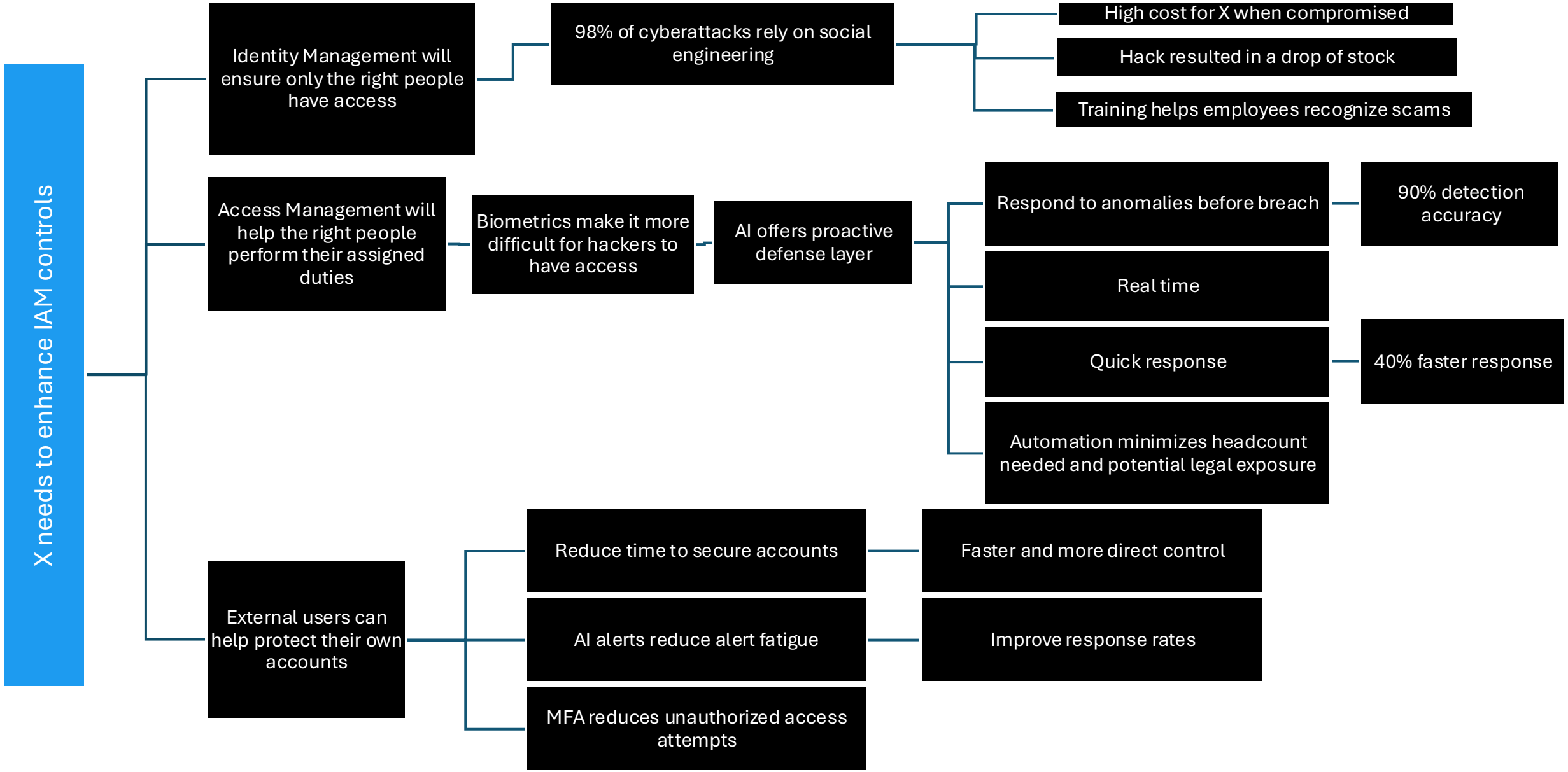
- Account lockdown
- Smart alerts
- Default security alerts

APPENDIX

APPENDIX: Issue Tree



APPENDIX: Hypothesis Tree



APPENDIX: Detailed Timeline

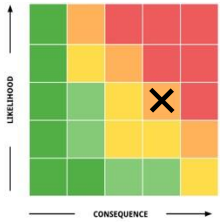
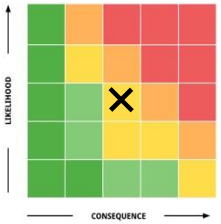
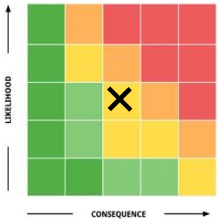
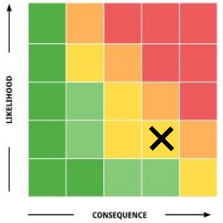
Activities	Months											
	Aug-20	Sep-20	Oct-20	Nov-20	Dec-20	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21
Identity Management												
Design phising simulations												
Design Social Engineering employee training												
Conduct employee training												
Conduct phising simulations												
Centralize employee identities into a single repository												
Expand Identify-Based Networking capabilities to remote workers												
Monitor identity management controls, update as needed												
Access Management - Authentication												
Security assessment												
Biometric authentication infrastructure setup												
Deploy Phishing-Resistant MFA (Pilot)												
Pilot Review & Refinement												
Full MFA Rollout												
Deploy AI-Driven Phishing Detection												
Implement Continous Behavioral Biometrics												
AI comprehensive Testing												
System monitoring and maintainance												
Access Management - Authorization												
Update Principle of Least Privilege access controls												
Redefine and update Role-Based Access Control												
Update Just-in-Time Access control												
Monitor authorization controls, update as needed												
External IAM												
Implement Instant Account Lockdown												
Launch AI-Driven Smart Alerts												
Enable Always-On Security Defaults												
Develop Rapid Recovery Systems												

APPENDIX: Detailed Financials

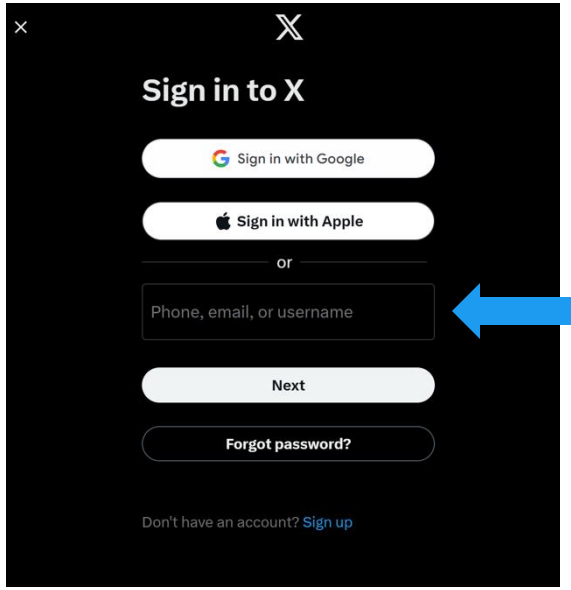
Period (e.g. Year)	0	1	2	3	4	5		
Net Cash Flows (NCF)	$(7,235,000)	$ 4,000,000	$ 4,000,000	$ 4,000,000	$ 4,000,000	$ 4,000,000		
NPV (Annual)	$(7,235,000)	$ 3,745,318	$ 3,506,852	$ 3,283,570	$ 3,074,503	$ 2,878,749		
ROI (Running Total)	-100%	-24%	4%	19%	28%	34%		
			Break Even					
Costs								
One-Time (Non-recurring)								
Cost of Consultants Hired to Assist Development[1]	$ 500,000							
Initial purchase price of Hardware Tokens(FIDO2) and Biometric	$ 200,000							
Infrastructure Setup and Configuration	$ 150,000							
AI-Driven Phishing Detection System Setup	$ 185,000							
Training users prior to going live	$ 200,000							
One-Time Costs per Period	$ 1,235,000						$ 1,235,000	Total One-Time Costs
Recurring								
AWS IAM Management Service (free for X)	$ -	$ -	$ -	$ -	$ -	$ -		
IT infrastructure costs of supporting the new software and hardv	$ 3,000,000	$ 3,000,000	$ 3,000,000	$ 3,000,000	$ 3,000,000	$ 3,000,000		
Salaries of IT or business employees, consultants/contractors involved with ongoing support of the solution as well as enhancements to it[1]	$ 200,000	$ 200,000	$ 200,000	$ 200,000	$ 200,000	$ 200,000		
Software and hardware licensing fees and/or upgrades	$ 2,500,000	$ 2,500,000	$ 2,500,000	$ 2,500,000	$ 2,500,000	$ 2,500,000		
Follow-up training and support costs	$ 300,000	$ 300,000	$ 300,000	$ 300,000	$ 300,000	$ 300,000		
Recurring Costs per Period	$ 6,000,000	$ 6,000,000	$ 6,000,000	$ 6,000,000	$ 6,000,000	$ 6,000,000	$36,000,000	Total Recurring Costs
Total One-Time and Recurring Costs per PeriodCosts	$ 7,235,000	$ 6,000,000	$ 6,000,000	$ 6,000,000	$ 6,000,000	$ 6,000,000	$37,235,000	Grand Total Costs
Cumulative Costs	$ 7,235,000	$13,235,000	$19,235,000	$25,235,000	$31,235,000	$37,235,000		
Benefits								
Cost avoidance								
Fines Avoidance		$10,000,000	$10,000,000	$10,000,000	$10,000,000	$10,000,000		
Total Benefits per Period	$ -	$10,000,000	$10,000,000	$10,000,000	$10,000,000	$10,000,000	$50,000,000	Grand Total Benefits
Cumulative Benefits	$ -	$10,000,000	$20,000,000	$30,000,000	$40,000,000	$50,000,000		

ROI	34%
NPV	$ 9,253,992
r	7%

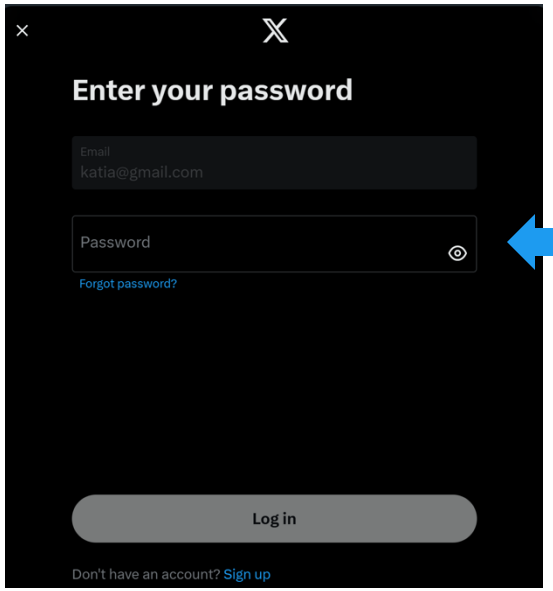
APPENDIX: Expanded Risks and Mitigations

Potential Risk	Risk Matrix	Mitigation Plan
Social Engineering is More Sophisticated Attackers are taking advantage of AI to target employees more effectively. The phishing emails look more credible and seem to originate from an internal source. Employees might still fall victim to these scams, which can lead to data breaches or other compromises of company information.		• Constantly update the training to adhere to current technology • Simulations should change routinely and adapt to any new practices of social engineering attacks • Require employees to use an internal directory to call back a caller to verify their identity
Employee Resistance Enforcing new security measures, such as biometric authentication, may result in employee resistance. Employees may feel the requirements of facial recognition or fingerprint scans is too intrusive and violates their privacy.		• Highlight privacy protections that X is taking to safeguard employees' data • Demonstrate the benefits employees will have, such as faster logins and better security in protecting sensitive information • Implement policies that automatically delete biometric data when they leave X
Evolving Regulatory Requirements As AI continues to develop, it is important that X adapts to the changes it poses to its security measures. However, regulatory requirements are continuously changing to catch up with newer disruptive technologies. X could risk being noncompliant and face legal repercussions due to changing regulatory demands.		• Perform regular audits to ensure the new IAM practices align with regulatory requirements • Automate compliance monitoring to flag non-compliant access patterns or data handling practices
Outdated Principle of Least Privilege Access HR will be required to be heavily involved so that PoLP remains updated with employees being terminated, hired, or moved around. However, it can be a time-consuming process so there may be periods of times that employees have too many privileges, or the wrong ones.		• Automated tools can reduce time of revoking and changing privileges • Prioritize employee changes and privilege access in HR department and IT to ensure faster response
Workflow Disruptions Just In Time (JIT) Access controls can delay work which can be problematic if the workflow is critical. JIT waits until the access is needed so it may take more time to handle critical situations.		• Implement predefined emergency access protocols that allow rapid access under specific conditions, with rigorous post-event audits • Allow limited, pre-approved JIT access for specific critical events, reducing the need for real-time approvals in emergencies

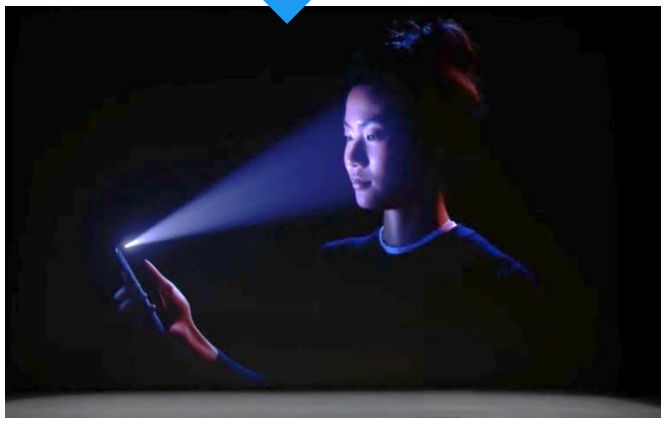
APPENDIX: Critical Terms for IAM



1. Identification
X is asking "Who are you?"



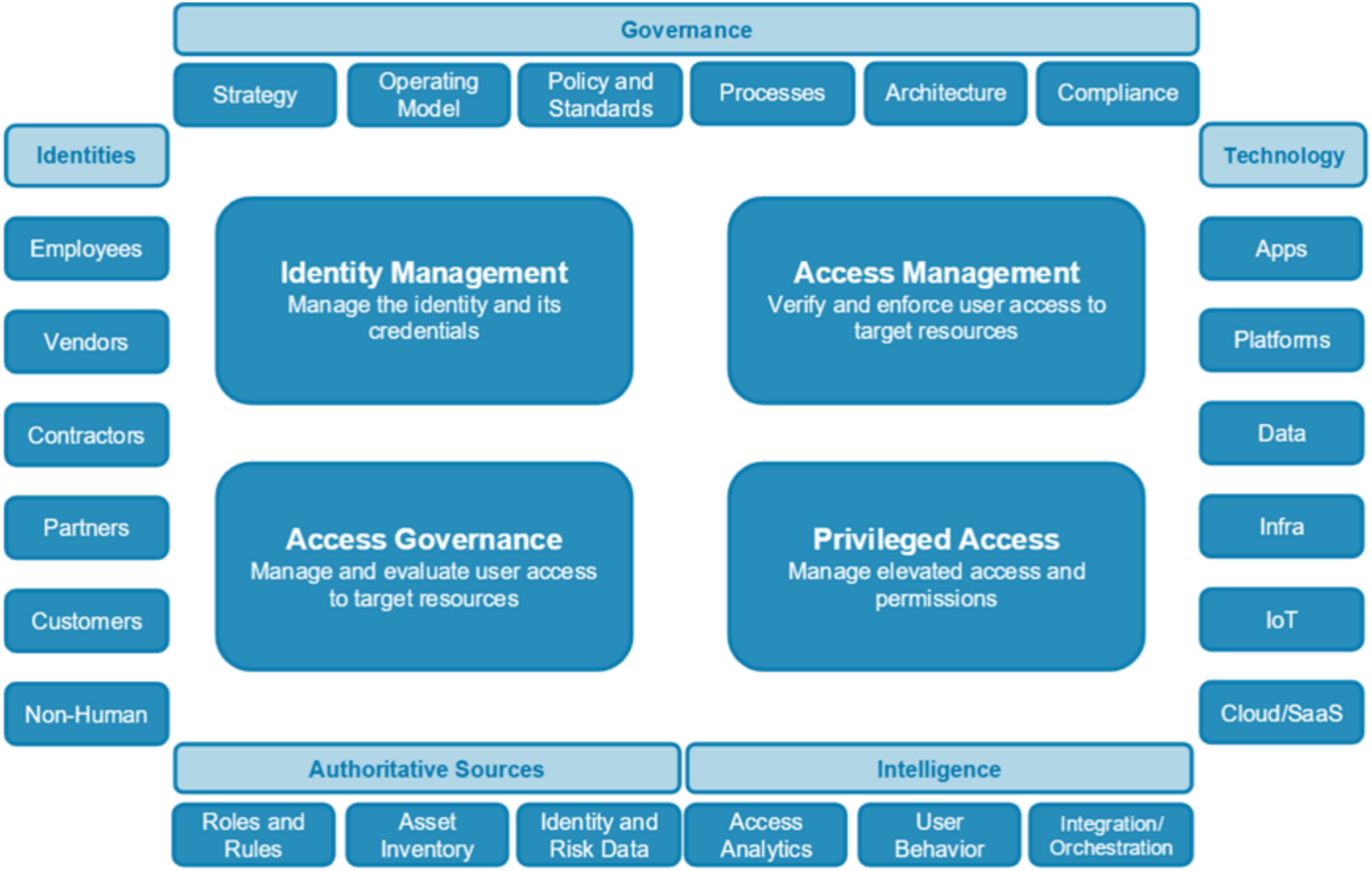
2. Authentication
X is asking "Can you prove you are who you are?"



3. Authorizations
X will give access to only the services the user has permission to access, which will vary by user role assigned

Source: IT GRC Class 2 Lecture Slides

APPENDIX: IT GRC IAM Overall IAM Landscape



Source: IT GRC Class 2 Lecture Slides

APPENDIX: Assumptions

- Twitter did not use AWS for IAM
- Twitter used AWS for basic infrastructure needs and it was not until after the hack that AWS became more involved
- Twitter used VPN for remote workers to be able to access their internal systems

Source: Amazon, Department of Financial Services

APPENDIX: Additional Sources

- The Hacker News
- Twitter Investigation Report
- How to access your X data
- How Twitter Survived Its Biggest Hack—and Plans to Stop the Next One