Driving TMHNA's Digital Transformation: Leveraging Integration, Cloud Services, and Advanced Analytics to Optimize Efficiency, Visibility, and Innovation Across Business Functions

Presented by:
3JK Solutions

Agenda

- Context
- Recommendation
- Timeline
- Financials
- Risks
- Conclusion

SolarWinds attackers operated undetected in the system for 14 months before being exposed

Breach Context

- In December 2020, SolarWinds experienced a highly sophisticated cyberattack- malicious actors inserted "SUNBURST" malware into the Orion software updates, which were then distributed to SolarWinds' clients, including government agencies and private companies
- This breach exposed critical weaknesses in SolarWinds' Identity and Access Management (IAM) practices and IT governance

Root Cause

- The SolarWinds breach occurred due to a combination of IAM failures, poor supply chain security, and a lack of IT governance oversight
- These root causes collectively enabled attackers to infiltrate and remain undetected within SolarWinds' systems, impacting high-profile clients and exposing critical security gaps

IT Governance and IAM

- How can SolarWinds transform its governance and IAM practices to prevent another breach, especially when its current policies failed to detect and mitigate risks within its supply chain and privileged access controls?

https://www.dfs.ny.gov/system/files/documents/2021/04/solarwinds_report_2021.pdf

Implementing a comprehensive IAM and governance framework will strengthen security and mitigate risks for SolarWinds

Comprehensive Overhaul of IAM Policies to Fortify SolarWinds' Security and Compliance

- Implementing a comprehensive IAM audit, strengthen access control policies, enforce multi-factor authentication (MFA), and implement continuous monitoring.
- Aligning these practices with NIST and COBIT frameworks will reduce vulnerabilities, enhance unauthorized access detection, and support compliance with industry standards.

Implementing Robust Governance and Auditing Practices to Enhance SolarWinds' Security Resilience

- Establishing clear roles, comprehensive policies, and rigorous risk assessments, alongside consistent internal and external audits.
- We aim to improve accountability, mitigate supply chain risks, and ensure adherence to security standards, enabling proactive threat detection and rapid incident response.

Enhancing SolarWinds' Security with Targeted Training, Strong Policies, and Dedicated Governance

- Implementing comprehensive employee training, robust IAM policies aligned with NIST and COBIT standards, and the creation of an IAM Governance Committee to oversee compliance, audits, and risk assessments.
- This approach ensures consistent enforcement of IAM practices and proactive risk management.

Creating Dedicated Oversight and Audit Teams to Strengthen IAM Compliance and Security at SolarWinds

- Formation of an IAM Governance Committee and an Internal Audit and Risk Management Team to regularly review IAM policies, conduct compliance audits, and monitor security risks.
- These teams will enhance oversight, ensure alignment with strategic goals, and provide transparency through regular reporting to the executive board.

SolarWinds must assess and revise the established IAM policies to improve organizational security

Comprehensive IAM Audit

Privileged Access Management (PAM):
Identifying accounts with elevated permissions and assessing for excessive privileges

API Security:
Reviewing API integrations for authentication, security, and restricted accesses

Account Lifecycle Management:
Evaluating user provisioning and de-provisioning to check if best practices were followed

Enhancing Access Control Policies

Role Based Access Control (RBAC):
Implementing a stricter RBAC framework to limit permissions based on job roles

Isolation of High-Risk accounts:
Isolating accounts with critical data to reduce risks

Enforce Least Privilege:
Redefining permissions for all users to ensure only the minimum privileges needed to perform tasks

Compulsory Multi-Factor Authentication (MFA)

Immediate Enforcement:
Implementing MFA for all users, especially highest privileged and high-risk user accounts

MFA Adoption Monitoring:
Tracking and reporting MFA adoption rates; setting a deadline for full adoption

Service Account Monitoring and Security

Identify and Secure Service Accounts:
Auditing service accounts used in automated processes and service builds
Credential Management:
Enforcing strong password policies for service accounts, along with periodic, required changes to passwords
Monitor Usage Patterns:
Continuous monitoring of service account activities

Ongoing Monitoring and Continuous Improvement

Log Integration and Analysis:
Implementing IAM-related logs in a Security Information and Event Management (SIEM) system to look for suspicious activities

Regular IAM Audits:
Scheduling periodic audits to review and update IAM policies

Expected Outcomes:

- Rapid reduction of IAM-related vulnerabilities
- Improved detection of unauthorized accesses
- Compliance with industry best-practices

Framework Alignment

- **NIST Cybersecurity Framework (CSF)**:

Leveraging "Identify", "Protect", & "Detect" functions

- **COBIT Framework:**

Aligning IAM policies with the business objectives

https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
https://delinea.com/blog/nist-800-53-security-privacy-privileged-access
https://rmcglobal.com/wp-content/uploads/2022/08/2020-SolarWinds-Hack-A-Case-Study-of-the-Russian-Cyber-Threat-July-2021.pdf

Establishing governance in the organizational structure and consistent internal and external auditing will prevent future attacks in the evolving threat landscape

Governance in Organizational Structure

Defining Clear Roles and Responsibilities

- **Accountability and Oversight:** Ensure cybersecurity is a shared responsibility across senior leadership, enhancing organization-wide accountability.
- **CISO and Security Leadership:** Appoint a dedicated CISO or equivalent leader to oversee strategic cybersecurity initiatives.

Establishing Policies and Procedures

- **Comprehensive Security Policies:** Develop and enforce policies for secure coding, data protection, and access controls.
- **Supply Chain Management Policies:** Implement policies to assess and monitor third-party security practices to mitigate supply chain risks.

Risk Management and Assessment

- **Enterprise Risk Management (ERM):** Conduct formal risk assessments to identify and prioritize cybersecurity risks.
- **Regular Risk Assessments:** Continuously evaluate and respond to emerging threats and the effectiveness of current controls.

Internal and External Auditing

Internal Audits:

- **Detection of Security Gaps:** Identify and address vulnerabilities in security controls and software development processes to mitigate risks before they can be exploited.
- **Compliance and Policy Adherence:** Ensure consistent adherence to internal cybersecurity policies, including secure coding, access controls, and monitoring.
- **Third-Party Risk Management:** Evaluate and mitigate risks associated with third-party vendors and supply chains to strengthen overall security.

External Audits

- **Independent Security Assessment:** Conduct impartial reviews to uncover vulnerabilities and blind spots that internal teams might miss.
- **Regulatory Compliance Assurance:** Verify adherence to relevant security and data protection regulations, fostering stronger cybersecurity practices.
- **Penetration Testing:** Simulate real-world attacks to expose weaknesses and prompt timely remediation of security vulnerabilities.

Changing Outcome with Governance in Organizational Structure and Internal/External Auditing

Risk Management

Enforcing supply chain security controls and regular risk assessments to detect vulnerabilities.

Policy Enforcement

Implementing strict controls over software updates with robust review processes.

Incident Response

Ensuring rapid detection and response to minimize breach impact.

Proactive Risk Detection

Identifying weaknesses in development practices and supply chain risks.

Compliance Checks

Ensuring adherence to security policies and secure coding standards.

Independent Assessments

External reviews to identify vulnerabilities and validate security practices.

https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management | https://www.cisa.gov/sites/default/files/2024 | 08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf | https://csrc.nist.gov/projects/incident-response
https://csrc.nist.gov/pubs/sp/800/161/r1/final | https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf | https://csrc.nist.gov/pubs/sp/1326/ipd

Training, policy, and charter recommendations will strengthen SolarWinds security framework

COBIT focuses on aligning IT processes with business goals and provides detailed governance and control objectives. SolarWinds can use COBIT to strengthen governance and ensure continuous oversight of IAM and cybersecurity policies

The **National Institute of Standards and Technology (NIST)** develops cybersecurity frameworks, like the NIST CSF, which guide organizations in managing and reducing cybersecurity risks.

Training

- **Objective:** Equip employees with the skills for enforcing robust IAM and governance practices.
- **Key Modules:**
    - Basic Cybersecurity Awareness: Risks, responsibilities, reporting.
    - Role-Based Training: Focus on RBAC, MFA requirements.
    - Advanced IAM Training: In-depth frameworks (NIST, COBIT), privileged monitoring.
    - Continuous Education: Monthly refreshers, breach simulations.
- **Delivery Methods:** Online modules, workshops, real-time simulations, assessments.

Policy

- **Objective**: Establish comprehensive IAM and governance policies aligned with NIST and COBIT.
- **Core Policies**:
    - Access Management: RBAC, least privilege enforcement.
    - Multi-Factor Authentication (MFA): Mandatory for high-risk accounts.
    - Auditing: Biannual IAM audits, internal and external checks.
    - Incident Response: Real-time monitoring, structured response.
    - Supply Chain Security: Third-party risk assessments.
- **Implementation**: Quarterly reviews by the IAM Governance Committee.

IAM Governance Committee Charter

- **Purpose**: Oversee and ensure IAM policy compliance and alignment with business goals.
- **Responsibilities**:
    - Develop, approve, and review IAM policies.
    - Conduct audits and manage risk assessments.
    - Report audit findings and emerging risks.
- **Membership Composition**: CISO, CIO, Legal, Compliance, Business Heads.
- **Reporting**: Biannual updates to the executive board; quarterly risk reviews.
- **Meeting Frequency**: Quarterly and as needed.

https://www.nist.gov/cyberframework
https://www.isaca.org/resources/cobit
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf
https://www.cisa.gov/resources-tools/resources/cybersecurity-workforce-training-guide

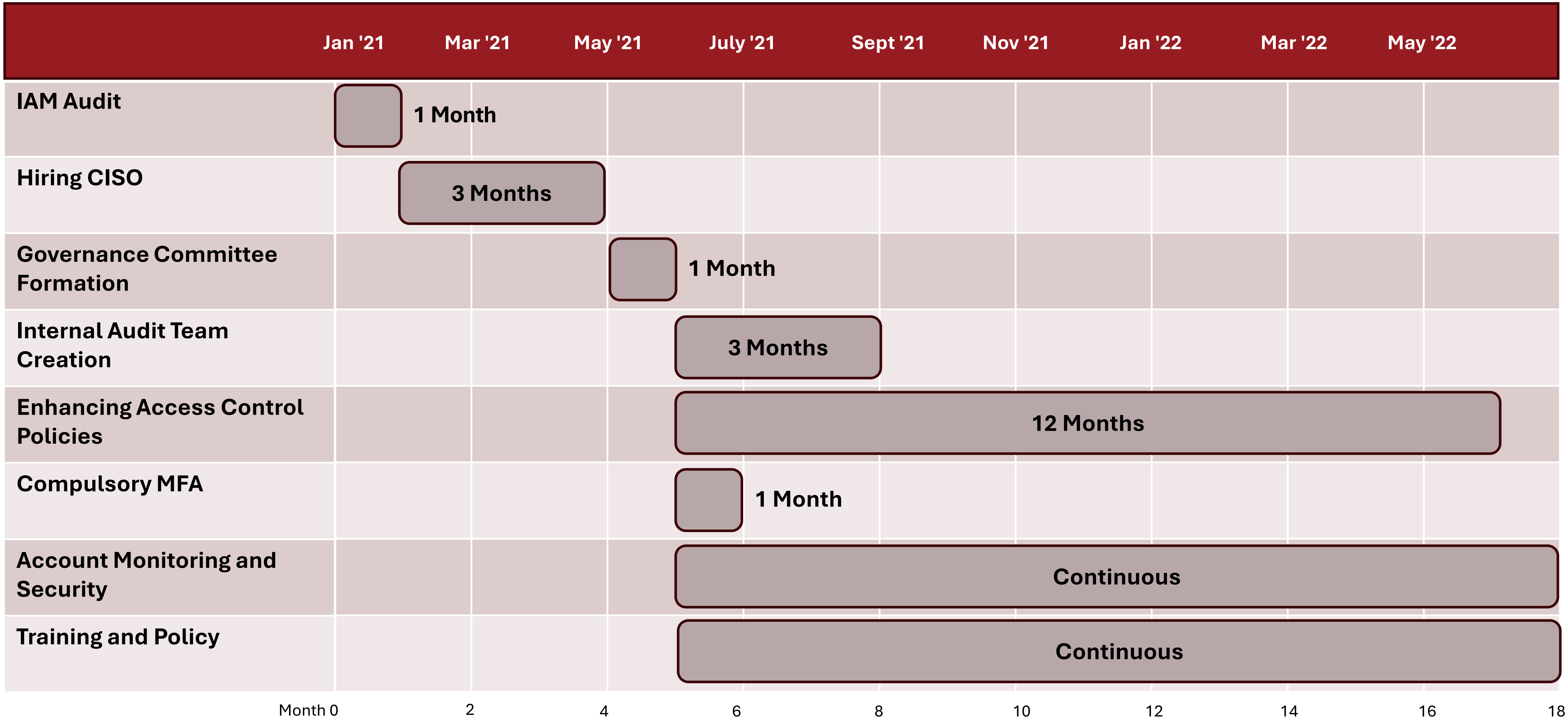
https://www.isaca.org/resources/cobit
https://www.cio.com/article/228151/what-is-cobit-a-framework-for-alignment-and-governance.html
https://www.cisa.gov/sites/default/files/2023-12/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.pdf

SolarWinds must strengthen their IT governance framework by implementing two new groups in the organization

	Purpose	Composition	Responsibilities	Reporting
IAM Governance Committee	The committee would oversee IAM policies, frameworks and audits, aligning IAM efforts with business and compliance requirements	Include senior leaders including the CISO, CIO, representatives from legal and compliance, and heads of key business units to ensure balanced decision-making	• Approve IAM policies and review them quarterly to ensure relevance and effectiveness • Oversee risk assessments focused on IAM to identify and address vulnerabilities exploited in the breach • Ensure IAM policies meet compliance standards (NIST CSF and COBIT) and align with SolarWinds's strategic goals	The committee should report IAM audit outcomes, policy updates and risk assessments to the executive board biannually to maintain transparency and secure top-level support
Internal Audit and Risk Management Team	Conduct biannual IAM audits, focusing on compliance, access control implementations, and privileged access monitoring	• Audit Manager- Leads IAM audits and ensures alignment with NIST CSF and COBIT frameworks • Cybersecurity Auditors- Evaluate IAM controls and identify compliance gaps • Risk Analysts- Access IAM-related risks and prioritize high-impact areas like 3rd party access • Data Analyst- Monitor access patters, detecting anomalies for investigation • IT Auditors- ensure technical implementation of IAM policies	• Perform biannual reviews focusing on PAM, MFA, RBAC, and third-party access • Maintain an IAM risk profile and recommend mitigations based on risk scores • Detect access anomalies, coordinating incident response • Recommend policy improvements based on audit result and evolving threats	Committee will provide quarterly reports to the IAM Governance Committee, summarizing audit findings, incident logs, and key recommendations. Biannual dashboard updates will present key IAM metrics and risk scores to the executive team, ensuring visibility into compliance status, emerging risks, and the effectiveness of ongoing IAM improvements.

https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF

The new IAM and governance framework will take 1.5 years to fully implement



IAM Audit	1 Month
Hiring CISO	3 Months
Governance Committee Formation	1 Month
Internal Audit Team Creation	3 Months
Enhancing Access Control Policies	12 Months
Compulsory MFA	1 Month
Account Monitoring and Security	Continuous
Training and Policy	Continuous

Investments in enhanced security measures will result in safeguards for the future

3JK SOLUTIONS

Estimated Costs for Implementing Recommendations

1. Internal Audit Team (5-7 Members)

- Estimated salary per auditor: **$80,000**
- Total annual salary for 5-7 auditors: **$400,000** to **$560,000**
- Training cost per auditor: **$5,000** annually
- Total annual training cost for 5-7 auditors: **$25,000** to **$35,000**

2. Updating IAM Systems

- Estimated range for IAM software acquisition: **$200,000** to **$500,000**
- Estimated implementation and customization services: **$100,000** to **$300,000**
- Estimated training costs for IT staff and end-users: **$50,000** to **$100,000**

3. Hiring a Chief Information Security Officer (CISO)

- Estimated CISO salary: **$250,000** to **$350,000**, including benefits and bonuses

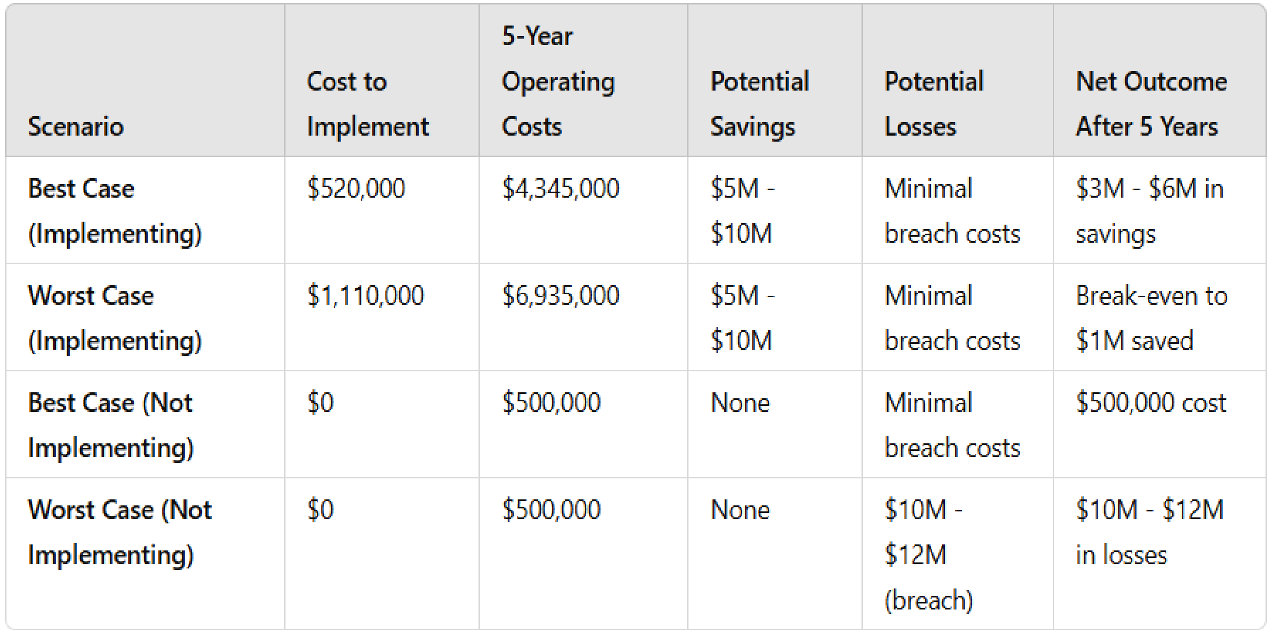
4. Additional Costs

- Estimated cost for third-party security audits per year: **$100,000** to **$200,000**
- Estimated annual maintenance and support costs: **$50,000** to **$100,000**

•**Total Annual Cost: $425,000** to **$595,000**
•**Total One-Time Cost: $350,000** to **$900,000**

Future Cost Benefits:

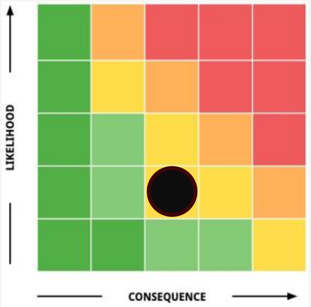
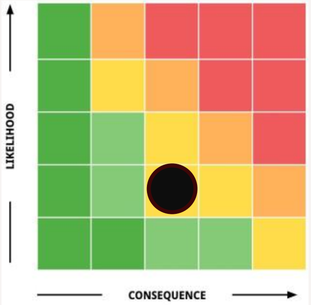
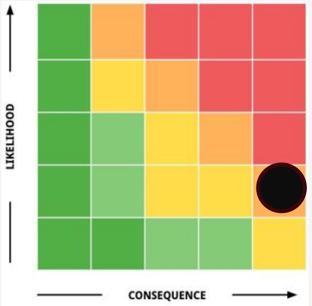
- **Reduced Risk of Data Breaches:** The average cost of a data breach in 2023 was **$4.45 million**.
- Implementing these measures can significantly lower this risk.
- **Regulatory Compliance:** Avoidance of fines and legal fees, potentially saving millions.
- **Operational Efficiency:** Streamlined processes leading to annual savings of **$100,000** to **$200,000**.
- **Reputation Management:** Maintaining customer trust and avoiding revenue loss.



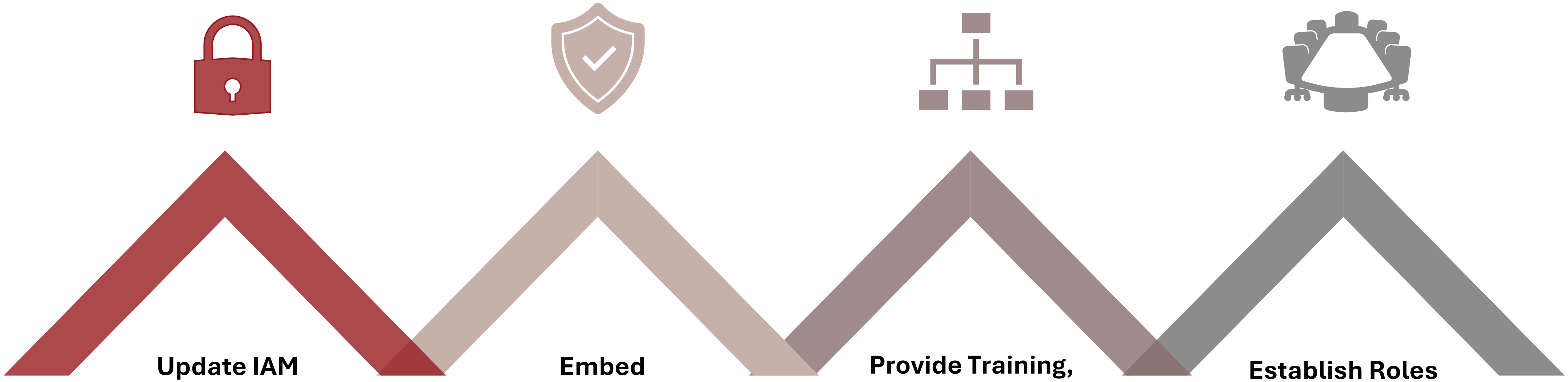
Scenario	Cost to Implement	5-Year Operating Costs	Potential Savings	Potential Losses	Net Outcome After 5 Years
Best Case (Implementing)	$520,000	$4,345,000	$5M - $10M	Minimal breach costs	$3M - $6M in savings
Worst Case (Implementing)	$1,110,000	$6,935,000	$5M - $10M	Minimal breach costs	Break-even to $1M saved
Best Case (Not Implementing)	$0	$500,000	None	Minimal breach costs	$500,000 cost
Worst Case (Not Implementing)	$0	$500,000	None	$10M - $12M (breach)	$10M - $12M in losses

Chief Information Security Officer Salary the United States – SalaryExpert | Internal Auditor Salaries by education, experience, location and more | Salary.com | Case Study: IAM Costs Cut Nearly in Half for Travel Services Provider – Simeio | achieving-cost-efficiencies-identity-and-access-management.pdf | Determining the Cost of an IAM Program - AIS Network

How can SolarWinds mitigate and avoid the risks of this undertaking?

Potential Risk	Risk Matrix	Mitigation Plan
Change Management: Inadequate planning or communication during the transition to new IT systems, processes, methodologies. Employees may not be adequately trained, resulting in errors, further risks, or poor performance.		Develop a clear communication plan that informs employees about the change, its importance, and how it will affect their roles. Providing thorough training sessions and ongoing support for all employees on new controls is essential. Additionally, rolling out changes in phases allows for adjustments based on feedback from early stages.
Employee Resistance: Emerge when employees resist adopting new IT systems and processes, particularly if they perceive them as burdensome or if they are not involved in the change process. This will lead to workarounds and employees feeling pushed out by management.		Involve employees early in the change process by gathering their input and addressing concerns to increase buy-in. Identifying key influencers within the organization who can promote the new systems, processes, and methodologies and provide support to their peers can also help. Introducing recognition or incentives for employees who adhere to the new systems, policies, and processes; support the change process effectively can further encourage compliance.
Improper Implementation: A key risk of poor implementation of these recommendations is the false sense of security within the organization. Security measures may appear robust but, if inconsistently enforced or inadequately monitored, critical vulnerabilities can go undetected. This can lead to severe breaches, data loss, regulatory penalties, reputational damage, and financial loss, as threats exploit overlooked gaps that proper governance and audits would have mitigated.		Implement continuous monitoring and auditing to quickly identify and address security gaps. Clear accountability and leadership oversight are crucial for consistent enforcement of policies and controls. Regular training ensures staff understand and adhere to security protocols. Independent assessments, such as external audits and penetration testing, provide unbiased validation of security measures. Finally, feedback loops and adaptive processes enable continuous improvement to strengthen security in response to emerging threats and past lessons.

SolarWinds must implement advanced IAM policies and undergo a governance overhaul to improve security in the organization



Update IAM and Policy

Evaluate IAM system and policies surrounding it.

Embed Governance

Establish governance in the organizational structure and begin internal audits,

Provide Training, Policies, & Established Chater

Develop training for updated policies, and a clear charter for the governance committee.

Establish Roles and Responsibilities

Hire audit team, CISO, and establish the governance committee.

APPENDIX

- Root Cause Analysis
- Issue Tree
- Additional Governance Guidelines
- Leveraging NIST CSF
- Leveraging COBIT Framework
- IT Operations: Current Issues and Implementations
- Potential Risks and Mitigation Plans for IT Control Implementation at Solar Winds
- Financials

Root cause analysis of the SolarWinds' data breach

1

Supply Chain Vulnerabilities in Software Development

- SolarWinds' software update process lacked robust security measures, which allowed attackers to compromise the Orion build environment.
- The "SUNBURST" malware was embedded directly into software updates, compromising clients' systems upon installation
- SolarWinds did not have sufficient checks to prevent malicious code from entering its supply chain, revealing a significant gap in supply chain security protocols

2

Inadequate IAM Controls

SolarWinds had weak IAM practices, including:

- Excessive Privileges: Many service and user accounts had more privileges than necessary, increasing the attack surface
- Lack of Role-Based Access Control (RBAC): Without strict RBAC, attackers could escalate privileges easily
- No Multi-Factor Authentication (MFA): SolarWinds did not enforce MFA consistently across privileged and high-risk accounts, making it easier for attackers to exploit single-factor authentication

3

Insufficient Monitoring of Privileged Accounts

- SolarWinds did not have adequate monitoring mechanisms for privileged accounts, which allowed attackers to maintain unauthorized access for months
- There was a lack of real-time monitoring and anomaly detection, particularly for privileged access activities within critical infrastructure, which delayed response and containment efforts

4

Lack of Executive Oversight and IT Governance

- There was minimal executive oversight over IAM policies and practices. IAM governance was not prioritized at the executive level, leading to poor enforcement and lack of accountability for IAM security
- This governance gap contributed to ongoing vulnerabilities in the IAM structure and hindered the company's ability to proactively address risks in supply chain security

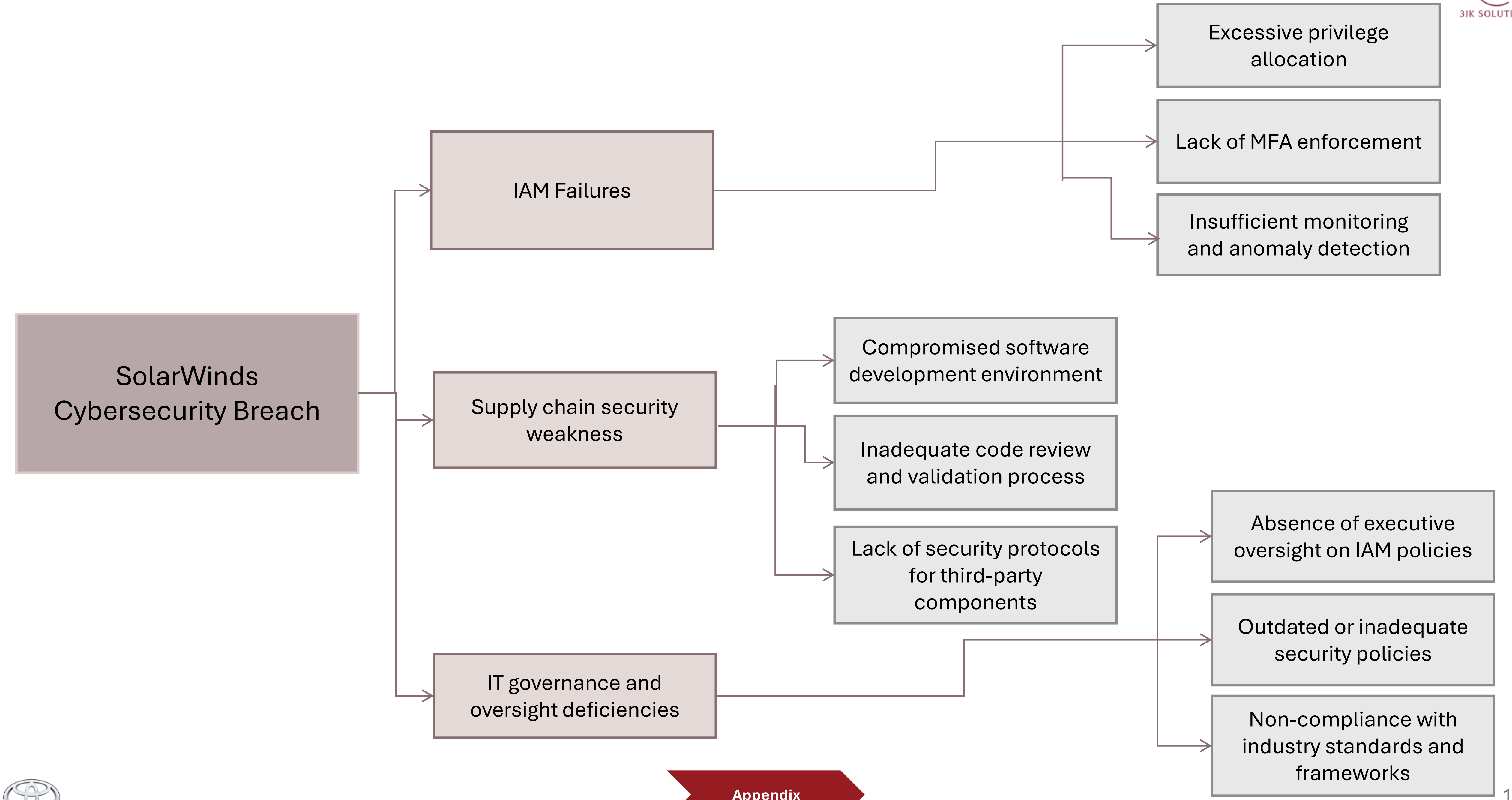
⚠

Contributing Factors

- Weak Password Management Practices: Reports indicate that an intern's insecure password, "solarwinds123," was publicly accessible for a period, exemplifying poor internal password management
- Delayed Incident Detection and Response: SolarWinds' cybersecurity response lacked the real-time detection mechanisms necessary to identify and contain the breach promptly. The extended delay in identifying suspicious access contributed to the breach's severity

Appendix

Root cause analysis: Issue Tree


SolarWinds Cybersecurity Breach
IAM Failures
Excessive privilege allocation
Lack of MFA enforcement
Insufficient monitoring and anomaly detection
Supply chain security weakness
Compromised software development environment
Inadequate code review and validation process
Lack of security protocols for third-party components
IT governance and oversight deficiencies
Absence of executive oversight on IAM policies
Outdated or inadequate security policies
Non-compliance with industry standards and frameworks

Appendix

Additional IAM governance roles and guidelines for SolarWinds' IT governance overhaul

Dedicated IAM Oversight Role

1. **Position**: Appoint an IAM Governance Officer who reports to the CISO and is responsible for ensuring IAM policies and practices are compliant, effective, and continuously improving.
2. **Responsibilities**:
    1. Coordinate IAM policy implementation, monitoring adherence across departments.
    2. Act as a liaison between IT, Compliance, and business units to ensure IAM policies are fully integrated into operational processes.
    3. Maintain a dashboard to track IAM-related incidents, remediation progress, and compliance status, providing regular updates to the IAM Governance Committee.
3. **Accountability**: The IAM Governance Officer would be responsible for enforcing role-based access control (RBAC), multi-factor authentication (MFA), and privileged account monitoring across all systems, with regular reviews to assess compliance and effectiveness.

Role-Specific IAM Policy Enforcement

1. **Executive-Level Oversight**: Require that any changes to privileged IAM roles (e.g., granting or modifying administrative rights) be reviewed by the CIO or another executive designee. This oversight will help mitigate risks associated with privileged access.
2. **Business Unit-Specific IAM Champions**: Designate IAM Champions within each department who report directly to the IAM Governance Officer. These champions are responsible for ensuring that employees in their respective units comply with IAM policies and complete necessary IAM training.

Leveraging the NIST cybersecurity framework (CSF)

NIST CSF is divided into 5 core functions and SolarWinds' should focus on specific functions and categories aligning with addressing IAM, supply chain security, and governance weaknesses

	Identify	Protect	Detect
Why	This foundational step ensures SolarWinds has a clear inventory of all assets, accounts, and third-party vendors, which is essential for identifying IAM risks and supply chain vulnerabilities	Protection mechanisms prevent unauthorized access to sensitive systems, which was a key vulnerability in the SolarWinds breach	Early detection of suspicious activities within privileged accounts or during software development could prevent prolonged exposure to attacks
How	• Implement Asset Management (ID.AM) to catalog all hardware and software assets, including Orion components and third-party libraries, to control access and assess vulnerabilities • Use Risk Assessment (ID.RA) to conduct regular risk assessments on IAM policies and third-party access controls, helping prioritize high-risk areas in their supply chain	• Enforce Identity Management, Authentication, and Access Control (PR.AC), focusing on implementing robust IAM policies, Multi-Factor Authentication (MFA), and Role-Based Access Control (RBAC) to limit access to critical systems • Apply Data Security (PR.DS) principles to protect data within the development environment, including securing privileged accounts and encrypting sensitive data to prevent unauthorized access	• Implement Anomalies and Events (DE.AE) detection systems, using real-time monitoring tools and behavior analysis to detect abnormal access patterns, particularly in privileged accounts • Adopt Continuous Security Monitoring (DE.CM) for the Orion build environment and third-party vendor activities to identify security events quickly

Appendix

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Leveraging the COBIT framework

COBIT focuses on aligning IT processes with business goals and provides detailed governance and control objectives. SolarWinds can use COBIT to strengthen governance and ensure continuous oversight of IAM and cybersecurity policies

	EDM (Evaluate, Direct, Monitor)	APO (Align, Plan, Organize)	DSS (Deliver, Service, Support)
Why	This ensures that executive leadership is actively involved in security governance, aligning IAM policies with business objectives and managing risks effectively	Establishing a structured, proactive approach to IAM policies and supply chain security	To ensure that IAM and security measures are applied consistently and effectively, especially in monitoring and incident response
How	• EDM02 (Ensure Benefits Delivery): Establish IAM policies that align with SolarWinds' business goals by focusing on risk management and value creation in security investments • EDM03 (Ensure Risk Optimization): Define specific IAM and cybersecurity risk tolerance levels, ensuring that governance decisions are made with clear risk mitigation strategies and accountability for IAM practices	• APO01 (Manage the IT Management Framework): Set up an IAM governance committee to create, monitor, and update IAM policies, ensuring continuous alignment with security standards • APO12 (Manage Risk): Conduct regular risk assessments and develop a risk register specifically for IAM and supply chain security, using this as a reference point for policy updates and improvement	• DSS05 (Manage Security Services): Implement dedicated IAM monitoring, logging, and alerting tools, especially for privileged access and third-party interactions, to enable immediate detection of unusual activities • DSS02 (Manage Service Requests and Incidents): Develop a rapid-response plan for IAM-related incidents, ensuring timely response and continuous improvement following incidents

Appendix

Governance in organizational structure and internal/external audits: current issues and implementations

	Governance Structure	Internal Auditing	External Auditing
Current State	• The board was responsible for overseeing the company's strategic direction and ensuring effective governance practices. In December 2020, Sudhakar Ramakrishna joined the board and later became President and CEO in January 2021. • The executive team managed daily operations and implemented board-approved strategies. Kevin Thompson is the President and CEO (until December 2020). Bart Kalsu is the Executive Vice President and Chief Financial Officer. Jason Bliss is the Executive Vice President, General Counsel, and Secretary. • While specific details about the Chief Information Security Officer (CISO) during this period are limited, the company had a cybersecurity framework in place. • SolarWinds maintained governance documents, including a Code of Conduct and Corporate Governance Guidelines, to guide ethical behavior and decision-making.	• Internal auditing structure exhibits notable deficiencies, particularly in its cybersecurity oversight. • The U.S. Securities and Exchange Commission (SEC) highlighted that the company lacked a dedicated Chief Information Security Officer (CISO) and had not established a comprehensive internal audit function focused on cybersecurity risks. • This absence of specialized leadership and structured internal auditing processes contributed to the company's vulnerability, as critical security gaps remained unidentified and unaddressed, ultimately facilitating the breach.	• Primarily focused on financial reporting and regulatory compliance, with limited emphasis on cybersecurity assessments. • The company engaged external auditors to review its financial statements and ensure adherence to accounting standards. • No publicly available evidence indicating that SolarWinds conducted comprehensive external cybersecurity audits or third-party evaluations of its software development processes and supply chain security during that period. • Lack of external scrutiny in critical areas may have contributed to the undetected vulnerabilities that were exploited in the attack.
Change	• Establish a dedicated Chief Information Security Officer (CISO) with clear authority and resources to oversee all cybersecurity initiatives. • Form cross-departmental security committees with representatives from IT, legal, compliance, risk management, and executive leadership. • Implement a robust risk management framework that prioritizes continuous assessment of supply chain security, software development practices, and third-party dependencies.	• Create a specialized internal audit team focused solely on cybersecurity risks. • Conduct regular, comprehensive audits of security controls, software development processes, and supply chain security. • Involve the Chief Information Security Officer (CISO) in audit planning, execution, and review. • Expand internal audits to regularly evaluate adherence to security policies, secure coding standards, and regulatory compliance.	• Regular external cybersecurity audits, including assessments of software development practices, supply chain security, and overall network defenses. • Engage external auditors with specific expertise in cybersecurity and supply chain risk management. • Include regular penetration testing and vulnerability assessments by external parties. • Mandate third-party assessments of the entire software supply chain to identify risks and enforce best practices. • Conduct ongoing external audits for compliance with evolving industry standards and regulations.
Impact	• This would centralize accountability for cybersecurity, ensuring proactive risk management, swift incident response, and alignment with best practices and regulations. • These committees would foster collaboration and coordination on cybersecurity policies, responses, and reviews, leading to a more unified and agile security approach. • This would enable SolarWinds to identify and mitigate vulnerabilities proactively, reducing the risk of exploitation through supply chain attacks.	• Enable continuous monitoring and auditing of security practices, ensuring vulnerabilities are detected and remediated promptly, reducing the risk of attacks. • Identify weaknesses and potential threats proactively, allowing for timely mitigation measures and strengthening overall defenses. • Ensures that cybersecurity audits align with strategic objectives, facilitating better risk management and accountability for security initiatives. • Maintains a high standard of security practices and reduce the risk of regulatory penalties due to non-compliance.	• Provide an unbiased evaluation of security measures, helping identify and address vulnerabilities before they can be exploited. • Ensure assessments are thorough and tailored to address current and emerging threats, providing more effective recommendations for security enhancements. • Simulate real-world attacks to identify and rectify weaknesses in systems and networks, improving the resilience of software products. • Minimize risks of compromise through third-party components, like the vectors exploited in the 2020 attack. • Remains aligned with best practices and up-to-date security protocols, reducing regulatory risks and improving trust with customers and stakeholders.

SolarWinds Investors
Norton Rose Fulbright
Securities and Exchange Commission

https://hbswk.hbs.edu/item/cold-call-how-solarwinds-responded-to-the-2020-sunburst-cyberattack
https://www.gao.gov/products/gao-22-104746

Appendix

https://www.cisa.gov/news-events/news/remediating-networks-affected-solarwinds-and-active-directorym365-compromise

https://www.arnoldporter.com/en/perspectives/advisories/2021/06/lessons-learned-from-the-solarwinds-cyberattack

Potential risks and mitigation plans for IAM and governance change at SolarWinds

Potential Risk:	Mitigation Strategy:
Compliance: Failure to meet key regulatory and industry security standards, such as supply chain security protocols or software integrity controls; result in serious consequences, including legal penalties, reputational damage, and loss of trust among clients and government agencies	Establish roles to oversee compliance and security activities, ensuring continuous updates and adherence to evolving regulations and best practices. Train staff on compliance requirements related to secure coding, software updates, and supply chain integrity to ensure consistent implementation.
Operational Risk: Implementing new IAM and Governance Structures can disrupt existing business processes, leading to potential downtime, reduced productivity, and operational inefficiencies. Poorly managed changes can lead to data integrity issues, affecting the accuracy and reliability of financial and operational data, which can impact decision-making and reporting.	Develop a phased implementation plan to minimize disruption. Schedule changes during off-peak hours and ensure thorough testing in a controlled environment before full deployment. Implement robust change management processes, including thorough testing and validation of changes before they are applied to production systems. Maintain detailed documentation and audit trails.
Security Risk: During the transition period, there may be increased vulnerability to cyber-attacks if security controls are not robustly implemented. This can lead to data breaches and loss of sensitive information. Without proper segregation of duties and access controls, there is a risk of insider threats, including unauthorized access and data breaches by employees or contractors.	Strengthen security controls during the transition period, including enhanced monitoring and incident response capabilities. Conduct regular security assessments and penetration testing. Implement strict access controls and segregation of duties. Regularly review and update access permissions. Conduct background checks and provide security awareness training for employees.
Financial Risk: Implementing/updating IAM and governance structures can be expensive, and there is a risk of cost overruns if the project is not well-managed. This can strain the company's financial resources. Allocating resources to implement may divert attention and funds from other critical business areas, potentially impacting overall business performance.	Develop a detailed budget and project plan with clear milestones and deliverables. Monitor expenses closely and adjust the plan as needed to stay within budget. Prioritize projects based on their impact on compliance and business operations. Allocate resources efficiently and consider hiring additional staff or consultants if necessary.
Reputational Risk: Any failures or breaches during the implementation phase can damage the company's reputation. Negative publicity can affect consumer and client confidence and customer trust. Inadequate controls can lead to data breaches, eroding customer trust and loyalty. This can result in customer attrition and loss of business.	Communicate transparently with stakeholders about the steps being taken to enhance IT controls and compliance. Develop a crisis communication plan to address any potential issues promptly. Implement strong data protection measures and communicate these efforts to customers. Provide regular updates on security and compliance initiatives to build trust.
Project Management Risk: Without clear project management, there is a risk of scope creep, leading to delays and increased costs. This can derail the project and impact its success. Insufficient expertise in implementing IT controls can lead to ineffective solutions and project failure. This can result in non-compliance and operational inefficiencies.	Define clear project scope and objectives. Change control processes to manage any changes to the project scope. Regularly review project progress and adjust as needed. Ensure that the project team includes individuals with the necessary expertise. Provide training and consider hiring external consultants to fill any gaps.

https://linfordco.com/blog/change-control-management/

https://www.paycor.com/resource-center/articles/overcoming-employee-resistance-to-change-in-the-workplace/#:~:text=70%25%20of%20change%20programs%20fail,%2C%20listening%2C%20timing%20and%20rewards.

Appendix

https://bridgepointconsulting.com/insights/it-controls-implementation-tips-benefits-steps/#:~:text=Assign%20Roles%20and%20Responsibilities:%20Clearly,the%20business%20requirements%20and%20objectives.

Financials

- ➢ The SolarWinds breach, which occurred in December 2020, had substantial financial and reputational impacts:

1. **Direct Costs**: SolarWinds reported spending approximately **$18 million** in immediate response costs, which included legal fees, incident response, and other direct expenses.
2. **Stock Value Impact**: Following the public disclosure of the breach, SolarWinds' stock dropped by around **25%**, which affected the company's market valuation significantly.
3. **Long-Term Costs**: Although exact figures are not fully disclosed, industry analysts estimate that the total long-term costs, including customer loss, regulatory fines, legal settlements, and increased security investments, could reach **upwards of $100 million** over time.
4. **Potential Lawsuits and Settlements**: SolarWinds also faced lawsuits and potential regulatory fines, adding further financial pressure.

- ➢ On average, large organizations experience **one data breach per year**. For high-risk sectors, such as finance and healthcare, this frequency can increase to **1-2 breaches per year**.

<u>Best-Case Scenario (Implementing Recommendations)</u>

Initial Investment:

- Cost to Build: $520,000 (best case) to $1,110,000 (worst case)
- Description: Initial setup costs for hiring a CISO, building an internal audit team, IAM updates, and training.

Annual Operating Costs (Years 1-5):

- Best Case: $965,000
- Worst Case: $1,585,000

Total Five-Year Costs (Including Initial Investment):

- Best Case: $4,345,000
- Worst Case: $6,935,000

Potential Savings & Benefits Over Five Years:

- Breach Prevention Savings: Avoiding 1-2 potential data breaches, each costing an average of $4.45 million (IBM's 2023 data breach report).
- Operational Savings: Improved efficiencies in IAM processes, estimated at $100,000 to $200,000 per year.
- Compliance Savings: Avoiding potential fines and legal costs, estimated at $500,000 to $1 million.

Net Financial Outcome After 5 Years:

- Best Case: $3 million to $6 million in net savings (from avoided breach costs, efficiencies, and compliance).
- Worst Case: Break-even to $1 million in net savings, factoring in worst-case costs and more limited risk avoidance.

<u>Worst-Case Scenario (Not Implementing Recommendations)</u>

Initial Costs:

•None: No immediate investment.

Annual Operating Costs (Years 1-5):

•Minimal security improvements and basic IAM updates: Estimated at $100,000 annually.

Total Five-Year Costs (Operating Only):

•Cost: $500,000 over five years.

Potential Losses Over Five Years (If Breach Occurs):

•Data Breach Costs: Potential 1-2 major breaches, each averaging $4.45 million in direct and indirect costs.

•Additional Costs:

- Reputation Damage: Loss of customer trust and business, potentially resulting in a revenue loss of $1 million to $3 million.
- Regulatory Fines and Legal Fees: Non-compliance fines and lawsuit settlements, estimated at $500,000 to $1 million.

Net Financial Outcome After 5 Years:

•Best Case: No major breaches, with only basic IAM upkeep, leading to net costs of $500,000.

•Worst Case: One or two significant breaches, resulting in a total financial impact of $10 million to $12 million (breach costs, reputation damage, and regulatory fines).

Appendix