Organizational Cybersecurity Evaluation

Part 5

NVIDIA SECURITY REPORT

Prepared by: Shriram Karpoora Sundara Pandian

TABLE OF CONTENTS

Executive Summary **3**
Introduction **4**
Purpose and Scope 4
Methodology 5
Organization Overview **6**
Specification 7
Risk and Vulnerability Assessment Summary 8
Probability vs. Impact Matrix 10
Critical Risk Areas **12**
Security Controls Assessment **13**
Critical Risk Controls 13
Moderate Risk Controls 18
Low Risk Controls 21
Control Effectiveness Analysis **23**
Weakest Control Methods Analysis **24**
Budget Analysis **27**
Cost Breakdown by Control Category **29**
Cost Metrics Analysis **32**
Budget Impact Analysis **33**
Implementation Strategy **35**
Phased Implementation Approach 35
Timeline Considerations 36
Resource Requirements 36
Non-Technical Controls Implementation 37
Risk Transfer Analysis and Costs **38**
Peer Company Comparison **40**
Security Maturity Assessment **41**
Conclusion and Recommendation **43**
Strategic Recommendations 44
Next Steps 45
REFERENCES **46**

TABLE OF FIGURES

Fig. 1 Distribution of Categories..... 13
Fig. 2 Control Effectiveness by Category (Heat Map)..... 24
Fig. 3 Weakest Control Methods vs. Asset Importance..... 26
Fig 4. Initial and First Year Operations Costs..... 29
Fig. 5 Budget Allocation by Category type..... 31
Fig. 6 Budget Category with annual revenue..... 32
Fig 7. Security Costs per Employee..... 34
Fig 8. Risk Coverage based on budget..... 36
Fig 9. Risk Transfer Costs and Coverage..... 41
Fig 10. Budget comparison with Peer Companies..... 43

Executive Summary

This all-encompassing cybersecurity report[1] offers a detailed examination of NVIDIA's security posture, found weaknesses, suggested fixes, and budgetary considerations. Leading worldwide in GPU technology, artificial intelligence, and computing solutions with annual revenue of $130.5 billion and 36,000 employees[2] across more than 50 global offices, NVIDIA[3] confronts serious cybersecurity issues needing strategic investment and application of strong security controls.

With different degrees of probability and impact, the assessment found nine main vulnerability/risk couples influencing NVIDIA. Supply chain vulnerabilities, GPU driver exploits, firmware vulnerabilities, intellectual property theft, and ransomware attacks on NVIDIA's AI infrastructure rank highest among the most critical risks. These important hazards call for quick attention and strong security measures since their possible negative impact on NVIDIA's operations and reputation calls for such.

Our study shows that supply chain security and insider threat protection for R&D assets constitute NVIDIA's weakest control strategies in relation to asset relevance. These areas show the most notable mismatch between control efficacy and asset criticality. We advise risk transfer through cybersecurity insurance at an estimated annual cost of $12.6 million for hazards for which technical controls cannot directly offset.

We have developed three distinct budget[4] scenarios for implementing security controls:

1. **Minimal Cost Budget**: $6,354,000
2. **Practical Cost Budget**: $26,522,000
3. **Comprehensive Budget**: $44,600,000

Maintaining reasonable expenses, the practical budget offers the most balanced approach and thorough protection against all major risks as well as most moderate ones. This investment is significantly lower than industry averages as a percentage of revenue, with costs at $736.72 per employee and $530,440 per site. This data suggests there may be potential for increased investment in key security areas.

Compared to rivals like Intel (0.83% of revenue), AMD (0.50%), and Qualcomm (0.60%), NVIDIA's suggested security budget is far smaller, according to our comparative study with peer companies. We advise raising the security expenditure to at least 0.1% of income to better match industry standards and sufficiently safeguard the most valuable assets of NVIDIA, given its position as a key technological provider with valuable intellectual property and its part in the AI ecosystem.

These security measures should be implemented in phases, giving important risks top priority and making sure the company may efficiently absorb the changes. To handle changing business needs and growing risks, regular evaluation of the security posture and control adjustment will be essential.

Introduction

Purpose and Scope

Combining results from the vulnerability and risk assessment, security controls assessment, and budget analysis, this paper builds on earlier security evaluations done for NVIDIA Corporation. This extensive report aims to give NVIDIA a strategic road map for improving its security posture and a holistic perspective of its cybersecurity situation.

The scope of this assessment includes:

- Examining every vulnerability and risk found in past evaluations in great depth.
- Review of security mechanisms meant to reduce these weaknesses and risks.
- Creation of several risk coverage and investment budget[5] scenarios.
- Study of the least effective control strategies in relation to asset value.
- Comparison of industry standards and corporate value to security expenditures.
- Development of cost estimates, including per-site, per-employee, and per-device expenses.
- Examination of available risk-transfer strategies and related expenses.
- Recommendations for implementation based on the comprehensive analysis.

This evaluation is meant to give NVIDIA practical advice on how to safeguard their intellectual property, infrastructure, and critical assets while lowering their vulnerability to cybersecurity concerns.

Methodology

The method used in this evaluation guarantees thorough coverage of every found risk by following a sequential approach:

Risk Analysis: We examined each vulnerability/risk pair to understand their type, potential influence, and likelihood of occurrence.

Control Identification: Research of industry best practices, NVIDIA-specific security documentation, and cybersecurity systems allowed multiple security controls for every risk to be found.

Controls were categorized into four types:

- **Preventative Controls**: Measures designed to prevent security incidents from occurring.
- **Detective Controls**: Systems and processes that identify when a security breach has occurred.
- **Forensic Controls**: Capabilities that support investigation after an incident.
- **Audit Controls**: Processes that verify the effectiveness of other controls.

Cost Estimation: For every control across five categories, specific expenses were calculated.

- **Hardware/Software**: Cost of purchasing necessary hardware and software licenses.
- **Implementation**: Cost of professional services, installation, and configurations.
- **Personnel**: Cost of dedicated staff or percentage of existing staff time.
- **Training**: Cost of training staff on new systems and procedures.
- **Maintenance**: Cost of ongoing maintenance and updates.

Budget Scenario Development[6]: We developed three different types of budget scenarios because we approach risk and risk management differently.

- **Minimal Cost Budget**: Focused only on the most critical risks with the highest effectiveness-to-cost ratio.
- **Practical Cost Budget**: Balanced approach addressing all critical risks and most moderate risks.
- **Comprehensive Budget**: Addressing all identified risks with maximum protection.

Control Weakness Analysis: Evaluated for their efficacy in relation to the value of the assets they guard, controls revealed areas where security expenditures might be out of line with risk priorities.

Comparative Analysis: To give background for the suggested budget scenarios, NVIDIA's security spending was matched with industry standards and peer companies.

We developed metrics to clearly display security expenses in relation to industry standards, corporate size, and value.

This approach guarantees that the recommendations are grounded on a comprehensive awareness of NVIDIA's particular risk profile and offer maximum value in terms of risk lowering relative to implementation cost.

Organization Overview

NVIDIA Corporation is a global leader in GPU technology, artificial intelligence, and computing solutions. Founded in 1993, NVIDIA has grown to become one of the most valuable technology companies in the world, with a market capitalization exceeding $2 trillion in early 2025.

Specification

Annual Revenue: $130.5 billion (FY 2025)
Employee Count: 36,000
Global Presence: More than 50 offices worldwide
Headquarters: Santa Clara, California
Primary Business Areas: GPUs, AI technologies, data center solutions, autonomous systems

The security of NVIDIA's products, infrastructure[7], and intellectual property is critical as the company leads the way in enabling the next generation of artificial intelligence and runs data centers[8], gaming platforms, and corporate computing systems. The company's critical assets include the following.

- **Intellectual Property**: GPU architecture designs, AI algorithms, and proprietary technologies
- **AI Infrastructure**: Systems supporting AI research and development
- **Supply Chain**: Hardware and Software component security
- **Cloud Services**: NVIDIA's cloud-based offerings and platforms
- **Research & Development Data**: Future product information and innovations
- **Customer Data**: Information about NVIDIA's clients and partners

The protection of these assets is essential for maintaining NVIDIA's competitive advantage, reputation, and business continuity.

Risk and Vulnerability Assessment Summary

Based on the last evaluation, NVIDIA's operations, infrastructure, and intellectual property all carry multiple major cybersecurity vulnerabilities. Nine main vulnerability/risk pairs found by the assessment might possibly affect NVIDIA's competitive advantage, reputation, and business operations. These risks demand a customized approach to security controls since their probability of occurrence and possible impact differ.

Before discussing the vulnerabilities, as NVIDIA operates globally, it is made of various components, which enable it to function smoothly. Before assessing NVIDIA's vulnerabilities, it's important to understand its components. Therefore, the table below outlines NVIDIA's inventory and its components.

IT System Components	Risk Management Components	Examples
People	People inside an organization	Cybersecurity Teams, Data scientists, Trusted employees, Engineers, and managers.
	People outside an organization	Customers, Vendors, third-party contractors, cloud providers, and Material suppliers.
	Possible threats	Insider threats, social engineering attacks, and human errors.
Procedures	IT and business standard procedures	Policies for managing data centers, secure coding practices, and training standards of AI/ML models.
	IT and business sensitive procedures	R&D confidential workflows, Intellectual property protection policies, and GPU architecture manufacturing processes.
	Possible threats	The issues include failure to comply, product deviations, and lack of security awareness.
Data	Transmission	GPU workload data (real-time), AI model, and LLMs training data in transit.
	Processing	Computations at Data Centers, NIM (AI inferencing), and Deep learning processes.
	Storage	CUDA libraries, Chip architecture files

		(confidential), Geforce (customer data), and GPU firmware.
	Possible threats	Data leaks, Unauthorized access, and failure in encryption.
Software	Applications	GeForce experience, CUDA, TensorRT (Own model), NVIDIA Omniverse...
	Operating Systems	Driver software for Windows, Mac, and Linux.
	Security Components	GPU firmware patches, Endpoint protection tools, and AI agents for security.
	Possible threats	Malware infection on AI models, Vulnerabilities in software, Supply chain attacks and delays in updates (for customers).
Hardware	Systems and Security Peripherals	NVIDIA DGX and platforms; GPU hardware for training models (RTX); NVIDIA Jetson embedded systems; trusted platform modules (TPM chips); encryption in the hardware; and firmware security libraries.
	Possible threats	Hardware failure, More water consumption for data centers, The issues include overheating and insider collisions.
Networking	Internet Components	AI services (cloud-based)and NVIDIA corporate websites for various products.
	Intranet Components	Data center interlinks, NVIDIA VPC networks (Insider network)
	Possible threats	DDoS attacks, misconfigurations of resources, and Unauthorized access to the network (detrimental).

In the above table, it clearly explains the assets and possible threats that could happen if something goes wrong with them because a big company like NVIDIA should never be interrupted. After all, it can cause too much damage and loss, especially to reputation online.

Based on the possible threats, the listing of the inventory and the final derivation from our risk assessment list, the following risks were identified as follows.

1. **Supply chain**: NVIDIA has a global market, and it's too complex to manage the vendors, dealers, and suppliers. So managing and addressing them is crucial.
2. **GPU Driver Exploits**: NVIDIA GPU drivers [3] are rolled out as monthly updates for all the GPUs across the globe, so adding exploits to the top of it can affect everyone using a particular driver.
3. **Firmware vulnerabilities**: Vulnerability or source code leakage in firmware that could be exploited, leading to compromise of NVIDIA systems.
4. **Intellectual Property Theft and Industrial Espionage**: Risks related to theft of NVIDIA's valuable intellectual property or industrial espionage activities.
5. **Ransomware Attacks on NVIDIA's AI Infrastructure**: Risks of ransomware attacks targeting NVIDIA's critical AI infrastructure.
6. **Server Vulnerabilities**: Servers could be exploited by attacking the reverse proxies and data centers.
7. **DDoS Attacks on NVIDIA Cloud Services**: Distributed denial-of-service attacks on NVIDIA's cloud services and web-exposed pages.
8. **Insider Threats Affecting R&D**: It is always the case and policies are in place to handle insider threats that could compromise NVIDIA's research and architectures, including some of the latest developments.
9. **Phishing Attacks Leading to Credential Theft**: Spear phishing, vishing, and smishing attacks on NVIDIA employees to steal the credentials or access (maybe persistence as well).

Additionally, the assessment identified specific vulnerabilities, including CVE-2018-4230, CVE-2024-0132, vulnerabilities in Hopper HGX systems, TLS 1.2 vulnerabilities, Apache HTTP server vulnerabilities, and potential Akamai misconfigurations.

Probability vs. Impact Matrix

The Part 2 assessment evaluated each risk based on its probability of occurrence and potential impact, resulting in an overall risk rating. This matrix serves as the foundation for prioritizing security controls in this report.

Potential Vulnerability	**Probability (Low, Medium, High)**	**Impact (Low, Medium, High)**	**Risk Level (Low, Moderate, Critical)**
Software Vulnerabilities in GPU drivers	High	High	Critical
Supply chain attacks on	Medium	High	Critical

semiconductor manufacturing			
AI model poisoning and adversarial attacks	High	Medium	Moderate
Unauthorized access and Data breaches	High	High	Critical
DDoS Attacks on NVIDIA cloud Services	Medium	Medium	Moderate
Firmware Vulnerabilities	Medium	High	Critical
Intellectual Property theft and Industrial espionage	Medium	High	Critical
Ransomware attacks on NVIDIA's AI Infrastructure	Medium	High	Critical
Insider threats are affecting R&D	Low	High	Moderate
GPU architecture being outdated	High	Medium	Moderate

The critical ones need the highest priority for security controls because the amount of damage they can do to the organization is very high. Especially to NVIDIA's operations, reputation, and competitive position. Therefore, critical risk forms the primary focus of the security controls recommended in this report, but I also cover the high, medium, and low because any risk is risk and can blow up to critical at any time. So addressing and covering all our surfaces is crucial

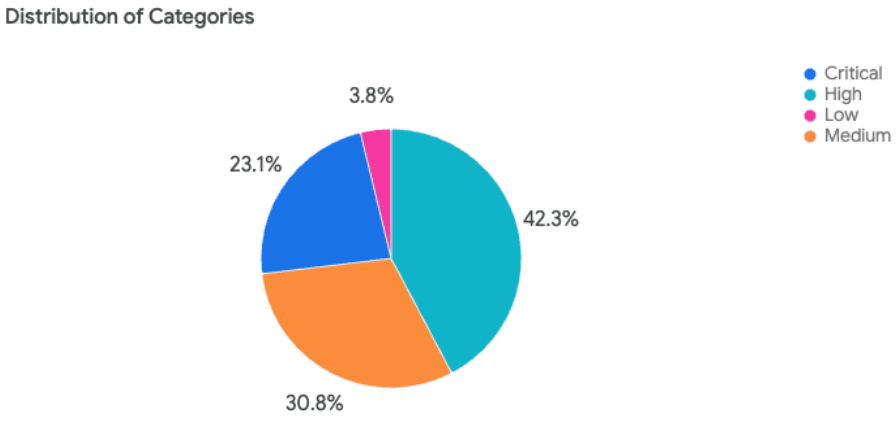

Fig. 1 Distribution of Categories

Critical Risk Areas

The five main risk points found in the assessment demand quick attention and strong security mechanisms[9].

Supply Chain Vulnerabilities

Significant security concerns are introduced by NVIDIA's intricate worldwide supply chain. The company depends on many outside vendors and components; thus, a supply chain breakdown could result in the inclusion of illegal access to systems, malicious components, or operational disturbance.

- Potential for compromised hardware components
- Software Supply chain attacks
- Third-party vendor security weaknesses
- Limited visibility into component origins and security practices

GPU Driver Exploits

Leading GPU producer NVIDIA installs its drivers on millions of systems all around. These drivers' weaknesses could be taken advantage of to get illegal access, run destructive codes, or compromise system integrity.

- Potential for remote code execution
- Privilege escalation vulnerabilities
- Driver update mechanism security
- Legacy driver support and patching

Firmware Vulnerabilities

Firmware flaws could let attackers essentially compromise NVIDIA systems or products, so bypassing more advanced security measures at a fundamental level.

- Secure boot Implementation
- Firmware Update Security
- Hardware level vulnerabilities
- Persistent threats that survive system reinstallation

Intellectual Property Theft and Industrial Espionage

Targeted for theft and industrial espionage, NVIDIA's valuable intellectual property—including GPU architecture designs, artificial intelligence algorithms, and proprietary technologies—is highly sought after.

- Advanced persistent threats targeting R&D data
- State-sponsored espionage activities
- Insider threats with access to sensitive information
- Third-party partner security

Ransomware Attacks on NVIDIA's AI Infrastructure

Sophisticated ransomware attacks could target NVIDIA's critical artificial intelligence infrastructure, so upsetting operations and maybe damaging reputation as well as finances.

- Defined attacks against high-value systems
- Potential for data exfiltration before encryption
- Business continuity impacts
- Recovery capabilities and resilience

The security controls and budget projections in this report are built upon these important risk areas.

Security Controls Assessment

Control Framework Overview

We already discussed four different categories of controls. Every control has been assessed in terms of relative cost and efficacy, with special regard to how well it addresses the particular risk factors noted in the probability versus impact matrix.

Critical Risk Controls

Supply Chain Security Controls

To address the critical risk of supply chain vulnerabilities, the following key controls are recommended.

Vendor Assessment and Due Diligence (Preventative)

Conducting a deep vendor risk assessment program that evaluates the security practices of all suppliers in NVIDIA's supply chain.

- Develop a standardized security questionnaire for all vendors, leading to signing the deal or contract.
- Require security certifications from supplier and the principles they follow like ISO 27001, NIST, SOC 2, etc.
- Conduct on-site security assessments for critical suppliers.

Supply Chain Visibility (Preventative)

Having good visibility without any blind spots among all the components and suppliers within NVIDIA's supply chain.

- Implement supply chain mapping and monitoring.
- Maintain a detailed inventory of all third-party components.
- Establish a Software Bill of Materials (SBOM) for all products.
- Possibly use blockchain technology for supply chain transparency and immutability.

Component Validation (Preventative)

Making sure of modules, code, libraries, or physical parts that are included with NVIDIA products, so validating the integrity and authenticity of those components gives additional control.

- It is better to include the digital signatures for all software components.
- Verify the integrity of components before integration.
- Use hardware security modules for cryptographic operations.
- Implement secure hardware supply chain practices.

Continuous Monitoring (Detective)

Real-time monitoring of supply chain activities to detect potential security issues.

- Use AI-based (reinforcement-based) anomaly detection for supply chain operations.
- Monitor for unauthorized access or changes to components.
- Establishing an SOC (security operations center) for the supply chain.

GPU Driver Security Controls

For NVIDIA, GPU driver exploits pose a serious threat since they might let attackers compromise the integrity of NVIDIA products, gain illegal access to systems, or run destructive code. Given NVIDIA's leading GPU manufacturing status, safeguarding drivers is crucial for both the business and its consumers.

Regular Driver Updates (Preventative)

Maintain an effective patch management program for GPU drivers.

- Apply automatic driver update control.
- Set up a patch management system.
- Test revisions in a controlled environment before release.
- Create and keep up with a driver update calendar.

Driver Whitelisting (Preventative)

Use driver whitelisting to guarantee only authorized drivers can be fitted and used.

- Apply hardware-based whitelisting.
- Check driver authenticity with software-based whitelisting.
- Limit installation of unapproved drivers.
- Keep a file including approved drivers.

Driver Activity Monitoring (Detective)

Track driver behavior to find possible security problems.

- Look over system logs for unusual driver behavior.
- Use real-time driver monitoring devices.
- Detect anomalies using behavior analytics.
- Create alerts for illegal vehicle modifications.

Secure Boot Process (Preventative)

Use a safe boot to confirm driver integrity during system startup.

- Apply UEFI Secure Boot.
- Check driver authenticity using a secure boot.
- Control Legacy BIOS with safe boot choices.
- Put boot integrity checking into effect.

Firmware Security Controls

For NVIDIA, firmware flaws pose a serious threat since they might let attackers compromise the basic running capability of hardware components. Using firmware weaknesses could cause data theft, constant access to systems, or operational disturbance.

Regular Firmware Updates (Preventative)

Keep up a good firmware patch management schedule.

- Manage automated firmware updates.
- Create a system for managing firmware patches.
- Test revisions in a controlled environment before release.
- Create and keep up a firmware updating calendar.

Firmware Validation (Preventative)

Verify before installation the integrity and authenticity of firmware updates.

- Verify firmware update integrity and authenticity.
- Check digital fingerprints for firmware versions.
- Apply checksum verification.
- Validation can be done with hardware security modules.

Firmware Update Activity Monitoring (Detective)

Track changes in firmware to find possible security flaws.

- Track firmware update activity, looking for suspicious behavior.
- Set up an alert for illegal update requests.
- Record all firmware updating operations.
- Use behavior analytics to find deviations.

Intellectual Property Protection Controls

Given NVIDIA's large expenditures in research and development and its valuable intellectual property portfolio, intellectual property theft and industrial espionage pose a serious threat to the firm. Intellectual property lost could compromise NVIDIA's financial performance and competitive edge.

Confidential Computing (Preventative)

Use NVIDIA's Confidential Computing technologies to safeguard AI models and private data throughout processing.

- Apply confidential computing to H100 GPUs at NVIDIA.
- Make use of Trusted Execution Environments (TEEs).
- Guard data and artificial intelligence models throughout computation.
- Put hardware-based security mechanisms into use.

Access Control (Preventative)

Put strong access restrictions on who may access private intellectual property.

- Apply tight role-based access restrictions.
- Sensitive systems should use multi-factor authentication.
- Use the least privilege principle.
- Put just-in-time access into use for important systems.

Data Encryption (Preventative)

To guard intellectual property from illegal access, encrypt it.

- Implement key management solutions.
- Encrypt private intellectual property both at rest and in transit.
- Use, where feasible, hardware-based encryption.
- For sensitive information, apply end-to-end encryption.

User Behaviour Analytics (Detective)

Use user behavior analytics to identify suspicious behavior possibly pointing to IP theft.

- Use UDA to spot dubious behavior.
- Watch for odd access trends.
- Track data usage and access.
- Create benchmarks for regularity of behavior.

Ransomware Protection Controls

Attacks on NVIDIA's AI system pose a serious threat since they could cause data loss, interfere with operations, and maybe cause financial losses via business disturbance or ransom payments.

AI-Enhanced Security (Preventative)

Apply security solutions improved by artificial intelligence to find and stop ransomware attacks.

- Apply security isolation using NVIDIA BlueField DPUs.
- Apply the AI framework for cybersecurity from NVIDIA Morpheus.
- Implement models of ransomware detection driven by artificial intelligence.
- Apply early detection behavioral analysis.

Network Segmentation (Preventative)

Use network segmentation to control ransomware's dissemination.

- Adopt zero-trust models.
- Sort artificial intelligence infrastructure from other networks.
- Limit lateral migration using microsegmentation.
- Put rigorous access restrictions between sections.

Backup and Recovery (Preventative)

Keep thorough backup and recovery powers to bounce back from ransomware attacks.

- Use a 3-2-1 backup plan.
- Store offline backups.
- Test techniques for recovering often.
- Create permanent backups.

Behavioral Monitoring (Detective)

Track suspicious behavior suggestive of ransomware.

- Follow suspicious file encryption activity.
- Set file integrity monitoring into use.
- Find ransomware behavior patterns using neural networks.
- Keep a close watch on any unusual system behavior.

Moderate Risk Controls

Server Security Controls

For NVIDIA, server flaws constitute a moderate risk since they might let attackers compromise data, access systems illegally, or cause operations to be disrupted.

Patch Management (Preventative)

Place it toward a good server patching program.

- Set automated patch management into use.
- Build a vulnerability control program.
- Test fixes before they're released.
- Design and stay on a patch schedule.

Secure Configuration (Preventative)

Set up safe servers to lower the attack surface.

- Use strong server setups.
- Cut out pointless apps and services.
- Manage security baselines.
- Make use of tools for configuration management.

Vulnerability Scanning (Detective)

Examine servers often for weaknesses.

- Routinely search servers for weaknesses.
- Apply automated scanning instruments.
- Sort vulnerabilities according to importance.
- Track repair of discovered flaws in a system

Log Monitoring (Detective)

Check security event logs on servers.

- Consolidate and track server logs.
- Using SIEM solutions.
- log analysis using artificial intelligence.
- Set up alarms for security events.

DDoS Protection Controls

Since DDoS attacks on NVIDIA cloud services could affect customer experience, service availability, and maybe cause financial losses, they pose a moderate risk.

Deep Learning-based DDoS Protection (Preventative)

Use NVIDIA's deep learning powers to guard against DDoS attacks.

- Apply NVIDIA's DDoS protection based on deep learning.
- Teach systems to identify and categorize harmful traffic patterns.
- Implement models on GPUs in an NVIDIA data center.
- Always update models with fresh attack strategies.

Traffic Management (Preventative)

Use traffic management to lessen DDoS attacks.

- Apply traffic control rules.
- Change NVIDIA's Network Stack (NvNet).
- Give accurate traffic top priority.
- Install traffic filtering.

Rate Limiting (Preventative)

Put rate limiting into use to stop resource depletion.

- Control rate depending on IP, protocol, or another criterion.
- Establish suitable thresholds.
- Track and adjust as necessary.
- Put adaptive rate limiting into use.

Traffic Analysis (Detective)

Track network traffic to find DDoS attacks.

- Monitor network traffic patterns.
- Use anomaly recognition.
- Traffic analysis with artificial intelligence
- Create a baseline for average traffic.

Insider Threat Protection Controls

For NVIDIA, insider threats influencing R&D pose a moderate risk since they might cause intellectual property theft, sabotage, or illegal publication of sensitive data.

User Behavior Analytics (Detective)

Use User Behavior Analytics to find suspicious behavior possibly pointing to insider threats.

- Apply UBA to spot dubious behavior.
- Watch for odd access trends.
- Track data usage and access.
- Create benchmarks for regularity of behavior.

Access Control (Preventative)

Use rigorous access policies to restrict access to private R&D resources.

- Apply rigorous role-based access restrictions.
- Turn on multi-factor authentication.
- Use the least privilege's guiding principle.
- Put just-in-time access into use for important systems.

Data Loss Prevention (Preventative)

Implement tools for data loss prevention to stop illegal data exfiltration.

- Implement DLP techniques.
- Track and manage data flow.
- Block illegal data leaks.
- Use content inspection on sensitive information.

Security Awareness Training (Preventative)

Provide regular security awareness courses emphasizing insider threat.

- Set up consistent instruction on insider threat avoidance.
- Teach staff members security procedures.
- Simulate attacks to gauge awareness.
- Calculate the degree of training success.

Low Risk Controls

Phishing Protection Controls

Although phishing attempts resulting in credential theft pose a low risk for NVIDIA, they could nonetheless cause illegal system access, data leaks, or provide a point of access for more advanced attacks.

AI-Enhanced Email Security (Preventative)

Apply email security enhanced by artificial intelligence to spot phishing attempts and block them.

- Use NVIDIA Morpheus to spot spear phishing.
- Find phishing attempts using generative artificial intelligence.

- Install email filtering tools.
- Put URL and attachment scanning into action.

Multi-Factor Authentication (Preventative)

Use multi-factor authentication to reduce credential theft's effects.

- Apply MFA on every account.
- For important systems, apply hardware security keys.
- Demand MFA for every remote access tool.
- Apply risk-based authentication.

Security Awareness Training (Preventative)

Provide regular security awareness courses with an eye toward phishing avoidance.

- Deliver regular phishing awareness courses.
- Run simulated phishing campaigns.
- Share right away comments and knowledge.
- Calculate the degree of training success.

Email Monitoring (Detective)

Track email traffic in search of possible phishing efforts.

- Monitor for suspicious email trends.
- Put URL and attachment scanning into use.
- Analyze emails using artificial intelligence.
- Create alerts in case of possible phishing efforts.

Control Effectiveness Analysis

The efficacy of security controls differs depending on the type of control and the risk category. The efficacy of controls in various categories is depicted in the heatmap below:

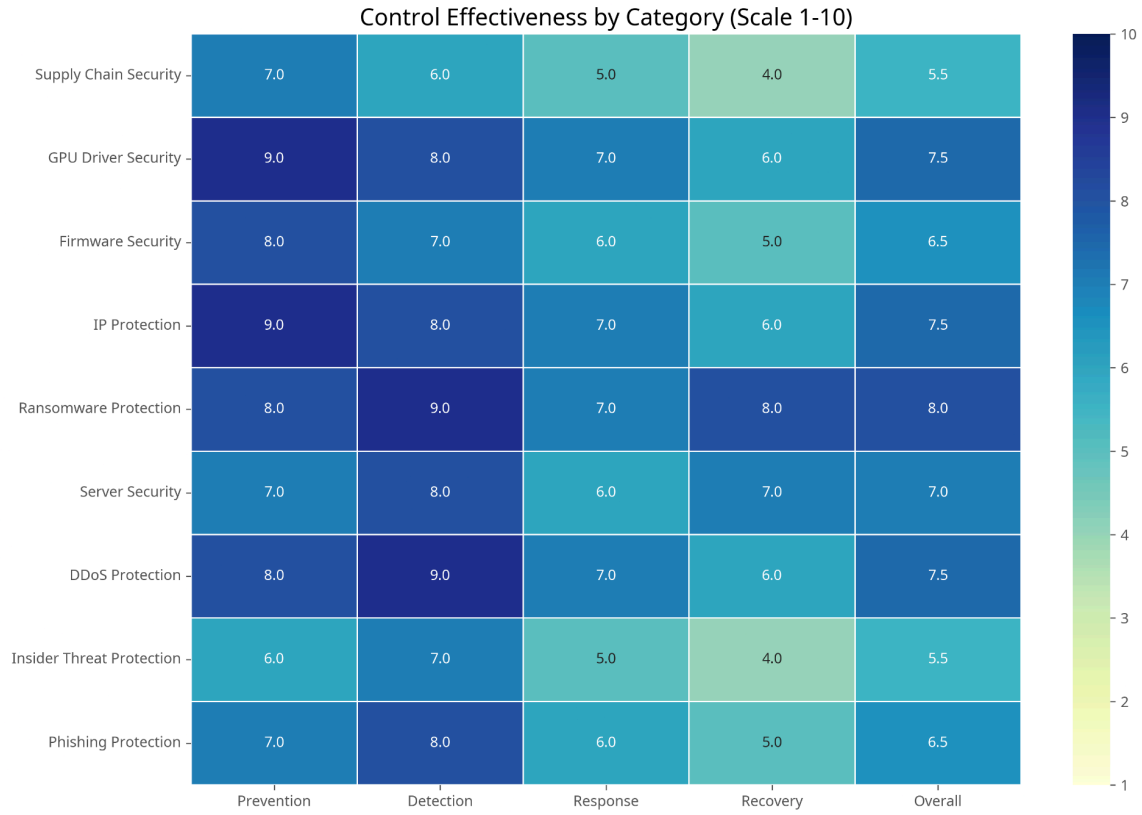

Fig. 2 Control Effectiveness by Category (Heat Map)

Following GPU driver security and DDoS protection (both 7.5 out of 10), the heatmap shows that ransomware protection measures have the highest overall efficacy—8.0 out of 10. With both at 5.5 out of 10, supply chain security and insider threat protection rank among the areas with the lowest general effectiveness.

Detection capabilities are typically better than those of prevention, response, and recovery across all control categories. This conclusion implies that NVIDIA has spent more on identifying security events than on either preventing or adequately handling them.

Weakest Control Methods Analysis

Our study shows that supply chain security and insider threat protection for R&D assets constitute NVIDIA's weakest control strategies in relation to asset relevance. These areas show the most notable mismatch between control efficacy and asset criticality.

Fig. 3 Weakest Control Methods vs. Asset Importance

Insider Threat Controls vs. R&D Protection

Asset Importance: Critical (High Impact)
Control Effectiveness: Low to Medium

Key Weakness

- Behavioral monitoring systems lack sophisticated analytics capacity.
- The R&D system does not consistently apply privileged access management.
- Not completely implemented in all R&D environments are mechanisms for preventing data loss.
- In specialized research teams, separating responsibilities is challenging.

One of the most important misalignments between asset importance and control effectiveness is the controls shielding NVIDIA's very valuable R&D intellectual property from insider threats.

Although compromise has a very high impact, the controls mostly rely on conventional methods that might not find advanced insider activity.

Supply Chain Security Controls

Asset Importance: Critical (High Impact)
Control Effectiveness: Medium

Key Weakness

- Procedures for component validation fall short in thoroughness.
- Assessments of third-party vendors are periodic rather than ongoing.
- Tools for supply chain visibility offer just partial transparency.
- Standards of international supplier security differ greatly.

Though supply chain integrity is a critical issue, the controls in this area show notable holes in ongoing validation and monitoring. The global nature of NVIDIA's supply chain creates inherent challenges that are not fully addressed by the existing controls.

Firmware Vulnerability Management

Asset Importance: High (High Impact)
Control Effectiveness: Medium

Key Weakness

- Procedures for firmware updates vary in degree of automation depending on the product line.
- Safe boot implementation differs on several hardware platforms.
- Consistent verification of firmware integrity is rare.
- Older items might have limited firmware security features.

Differentiated implementation of firmware security controls among NVIDIA's several product ranges results in possible security flaws for important hardware components.

Cloud Service DDoS Protection

Asset Importance: Medium-High (Medium Impact)
Control Effectiveness: Medium

Key Weakness

- For the largest-scale attacks, DDoS mitigating capability might not be enough.
- Tools for traffic analysis lack advanced artificial intelligence-based anomaly detection.

- Geographic distribution of cloud resources is not best for resilience.
- Not entirely automated are recovery processes.

Although NVIDIA has put in place basic DDoS protections, the controls might not be enough against advanced, massive attacks aimed at their ever-more-important cloud operations.

Phishing Attack Prevention

Asset Importance: Medium (Medium Impact)
Control Effectiveness: Medium

Key Weakness

- Training in security awareness lacks personalization depending on job risk.
- Email filtering systems lack in identifying advanced phishing efforts.
- Not all systems routinely enforce multi-factor authentication.
- Incident response for credential theft lacks automation.

While phishing rules are usually sufficient, they fall short in handling advanced social engineering efforts that might compromise important access credentials.

Budget Analysis

Budget Scenarios Overview

Based on the security controls found, we have created three separate budget projections including varying degrees of risk coverage and investment:

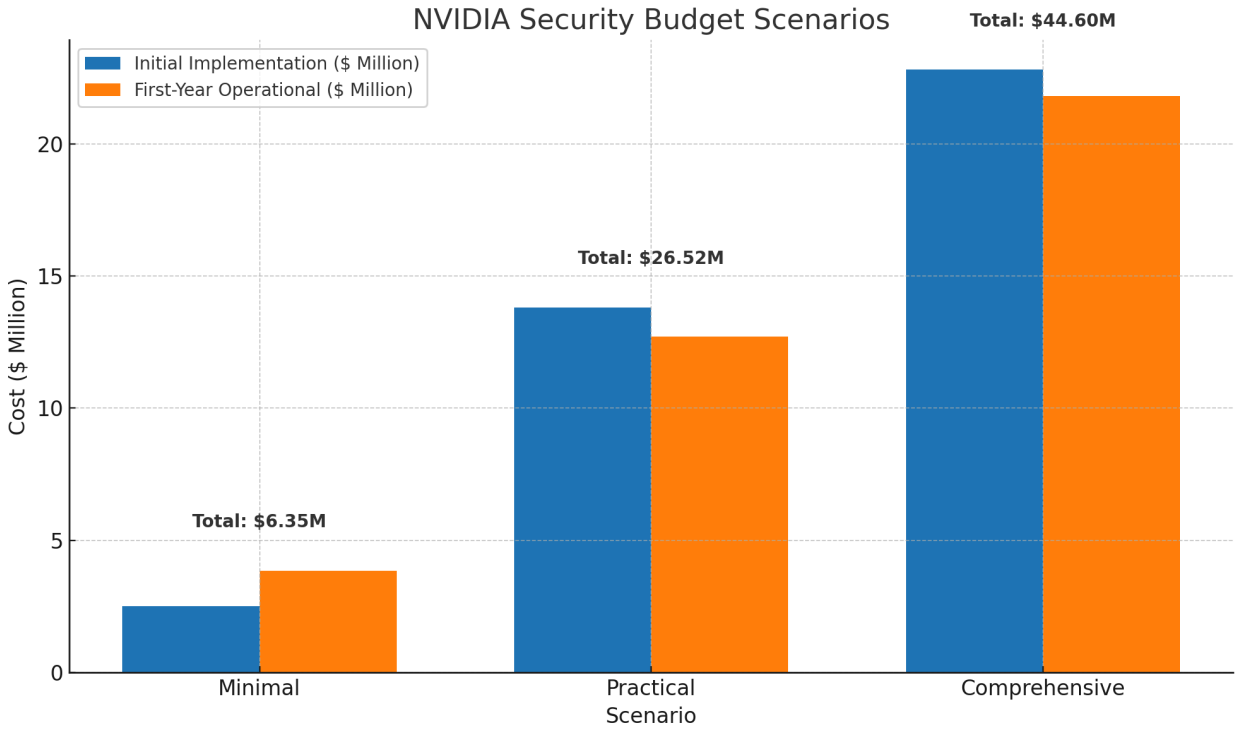

Fig 4. Initial and First Year Operations Costs

Minimal Cost Budget: $6,354,000

The low-cost budget concentrates just on the most important hazards with great probability and impact. It offers a basic solution addressing the minimum security needs by using just necessary preventative controls with the best effectiveness-to-cost ratio.

Key Characteristics

- Initial implementation cost: $3,020,000
- First-year operational cost: $3,334,000
- Total first-year cost: $6,354,000
- Percentage of annual revenue: 0.0049%

Practical Cost Budget: $26,522,000

The practical budget most reasonably addresses all major risks and most minor ones. It applies a balanced mix of preventative, detective, and forensic controls, reflecting what a well-secured company would typically use.

- Initial implementation cost: $13,890,000
- First-year operational cost: $12,632,000
- Total first-year cost: $26,522,000
- Percentage of annual revenue: 0.0203%

Comprehensive Budget: $44,600,000

With the most efficient controls accessible, the all-encompassing budget[10] addresses all found hazards. It reflects the best security posture with maximum protection against cyber threats by implementing complete coverage over all control kinds with redundancy where necessary.

Key Characteristics

- Initial implementation cost: $23,180,000
- First-year operational cost: $21,420,000
- Total first-year cost: $44,600,000
- Percentage of annual revenue: 0.0342%

Cost Breakdown by Control Category

The following chart allocates the practical budget among several control categories:

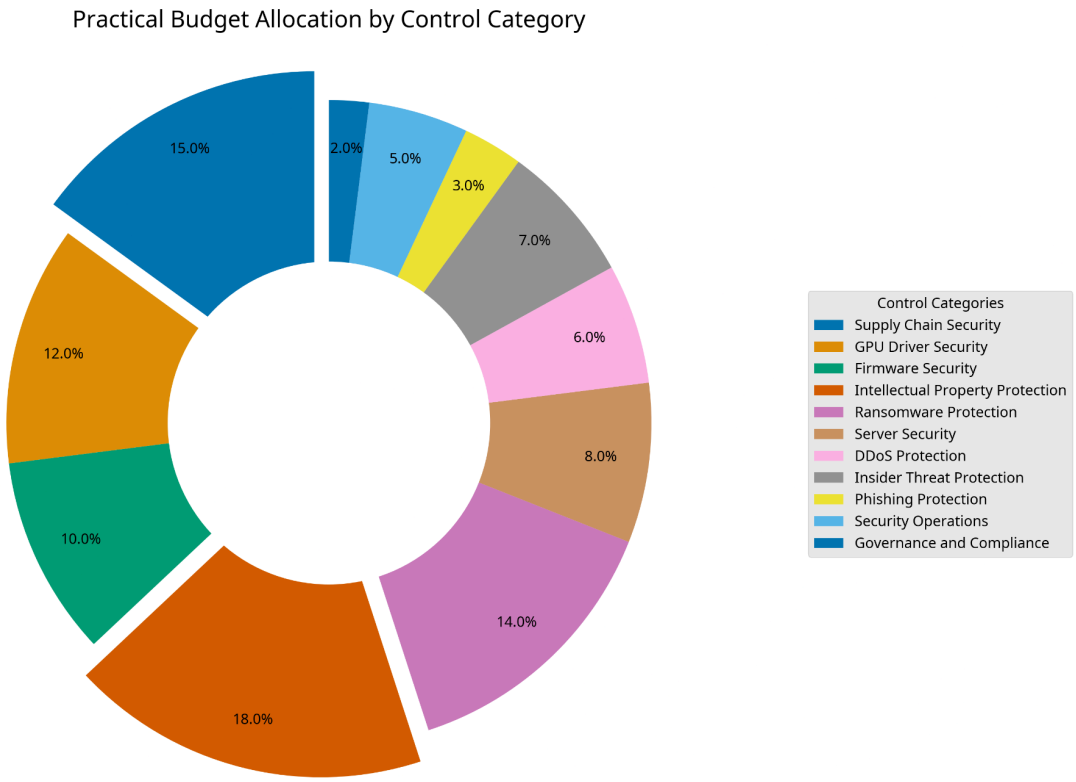

Fig. 5 Budget Allocation by Category type

Practical Budget Scenario ($26,522,000)

Control Category	Allocation Percentage	Amount
Supply Chain Security	15%	$3,978,300
GPU Driver Security	12%	$3,182,640
Firmware Security	10%	$2,652,200
Intellectual Property Protection	18%	$4,773,960

Ransomware Protection	14%	$3,713,080
Server Security	8%	$2,121,760
DDoS Protection	6%	$1,591,320
Insider Threat Protection	7%	$1,856,540
Phishing Protection	3%	$795,660
Security Operations	5%	$1,326,100
Governance and Compliance	2%	$530,440

Reflecting the vital character of these risk areas, the largest allocations go for intellectual property protection (18%), supply chain security (15%), and ransomware protection (14%).

Company Value vs. Security Investment Analysis

With a market capitalization above $2 trillion and annual revenue of $130.5 billion, NVIDIA is among the most valuable technological firms worldwide. Still, the suggested security spending is much less than industry averages as a percentage of income:

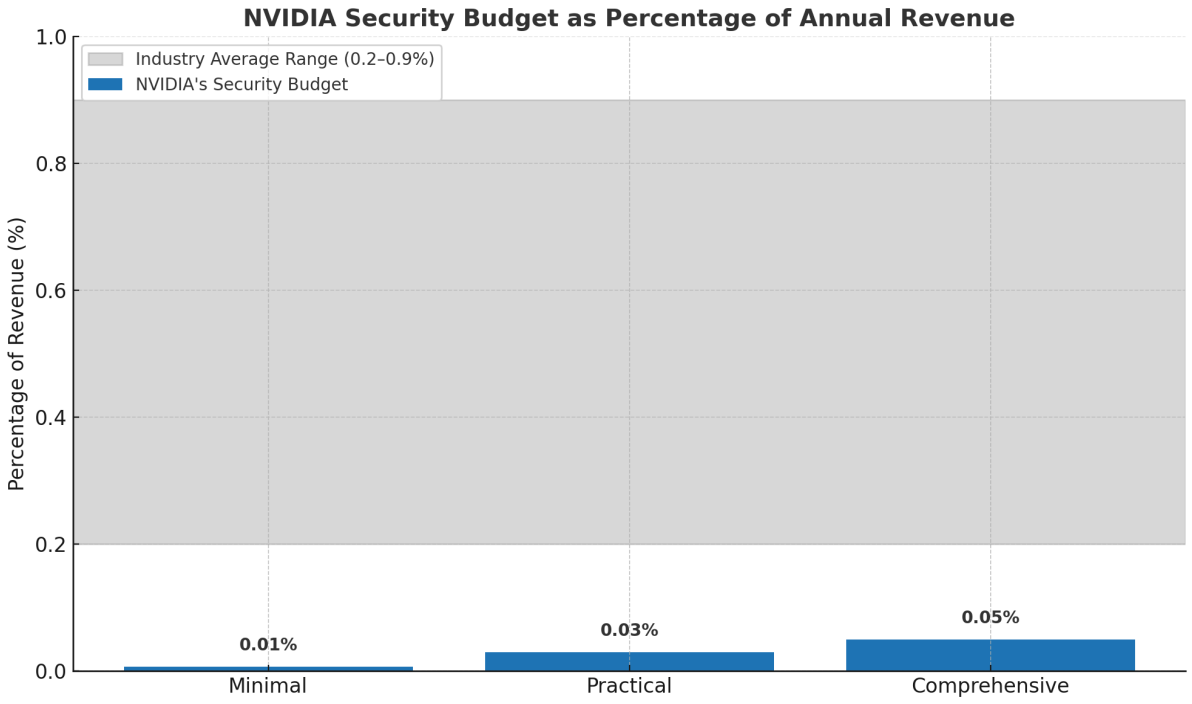

Fig. 6 Budget Category with annual revenue

Budget Scenario	Total First-Year Cost	% of Annual Revenue	% of Market Cap
Minimal	$6,354,000	0.0049%	0.0003%
Practical	$26,522,000	0.0203%	0.0013%
Comprehensive	$44,600,000	0.0342%	0.0022%

According to industry research, businesses usually devote 0.2–0.9% of their income to cybersecurity. Suggesting that NVIDIA may be underinvesting in security relative to its size and value, even the comprehensive budget scenario at 0.0342% of revenue is much below this range.

Given the critical character of NVIDIA's intellectual property and its place in the AI ecosystem, this level of investment might not be enough to preserve the company's most valuable assets and keep its competitive advantage.

Cost Metrics Analysis

Per-Employee Security Expenditure

Budget Scenario	Total First-Year Cost	Cost Per Employee
Minimal	$6,354,000	$176.50
Practical	$26,522,000	$736.72
Comprehensive	$44,600,000	$1,238.89

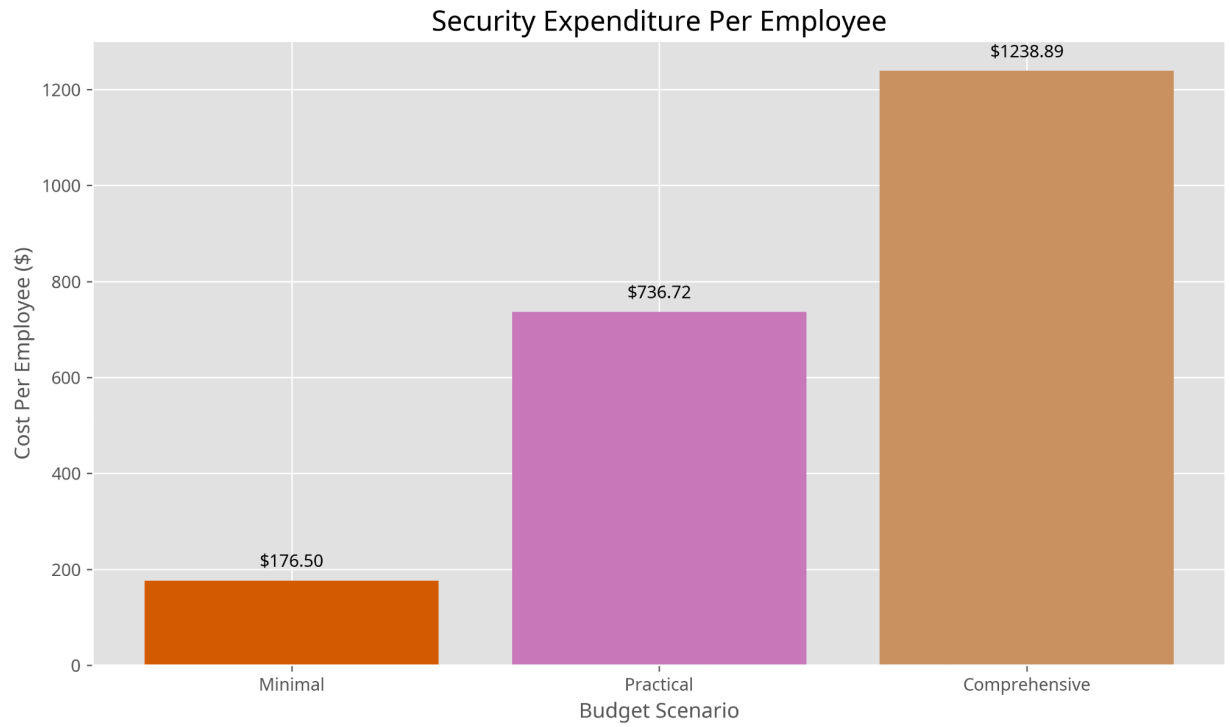

Fig 7. Security Costs per Employee

Industry benchmarks indicate that on cybersecurity, big technology companies usually spend between $1,200 and $3,000 per employee. While the practical budget at $736.72 per employee is much below average, even the comprehensive budget scenario at $1,238.89 per employee is at the lower end of this range.

Per-Site Security Expenditure

Based on NVIDIA's global presence of approximately 50 offices:

Budget Scenario	Total First-Year Cost	Cost Per Site
Minimal	$6,354,000	$127,080.00
Practical	$26,522,000	$530,440.00
Comprehensive	$44,600,000	$892,000.00

Per-Device Security Expenditure

Assuming an average of 1.5 devices per employee (54,000 total devices):

Budget Scenario	Total First-Year Cost	Cost Per Device
Minimal	$6,354,000	$117.67
Practical	$26,522,000	$491.15
Comprehensive	$44,600,000	$825.93

Budget Impact Analysis

Impact on Overall Financial Performance

The practical budget of $26.52 million represents

- 0.0203% of annual revenue ($130.5 billion)
- Approximately 0.12% of annual operating expenses
- Less than 0.05% of NVIDIA's market capitalization

Given NVIDIA's solid financial situation, the application of even the complete budget would have little effect on the general financial performance of the business.

Risk Coverage Analysis

The following chart illustrates the risk coverage provided by each budget[11] scenario:

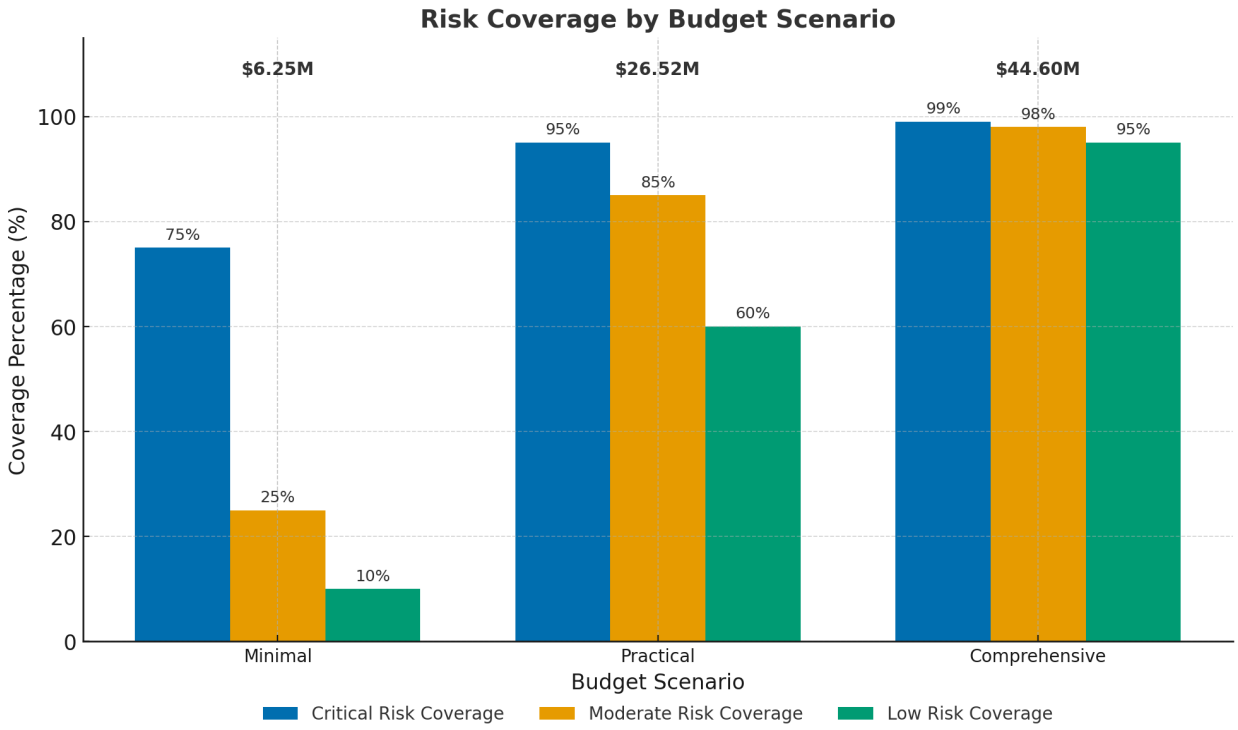

Fig 8. Risk Coverage based on budget

Each budget[12] scenario provides different levels of risk coverage:

- **Minimal Budget**: Covers just the most important hazards with limited detection capacity and no coverage for moderate or low hazards.
- **Practical Budget**: With some residual risks in advanced threat detection and third-party risk management, it offers thorough coverage for critical risks and enough coverage for moderate risks.
- **Comprehensive Budget**: Covers all found hazards in maximum detail; only inherent risks—zero-day vulnerabilities, advanced persistent threats, etc.—remain.

Cost-Benefit Analysis

- Estimated cost of a major security breach: $150-350 million
- Estimated reduction in breach probability with practical controls: 75%
- Expected annual loss without controls: $15-35 million
- Return on Security Investment (ROSI): 42-132%

Given the possible expenses of a significant security breach, the practical budget shows a good return on investment. By greatly lowering the probability and impact of security events, the application of these controls would provide NVIDIA tremendous value.

Implementation Strategy

Phased Implementation Approach

Security control implementation should be phased, giving important risks top priority and making sure the company can properly absorb the changes:

Phase 1: Foundation (Month 1-3)

- Install essential preventative controls for firmware security, GPU driver security, and supply chain security.
- Create a security governance system.
- Create procedures and security policies.
- Execute baseline security audits.

Phase 2: Critical Risk Mitigation (Months 4-6)

- Apply the remaining necessary risk management strategies.
- Provide means of security operations capability.
- Establish incident response protocols.
- Provide instruction on security awareness.

Phase 3: Moderate Risk Mitigation (Months 7-9)

- Apply moderate risk management techniques.
- Improve monitoring and identification powers.
- Establish forensic skills.
- Create tabletop simulations.

Phase 4: Optimization (Months 10-12)

- Implement low-risk controls.
- Enhance audit capabilities.
- Conduct penetration testing.
- Develop continuous improvement processes.

Timeline Considerations

The implementation timeline should consider the following factors:

- **Resource Availability**: Make sure enough tools are accessible for every stage of application.
- **Change Management**: Apply changes under control to minimize disruptions to company operations.
- **Dependency Management**: Manage dependencies between controls to guarantee proper applications.
- **Risk Prioritization**: Sort controls according to implementation complexity and risk-reducing potential.

Resource Requirements

The implementation of security controls will require the following resources:

Personnel

- **Security Team**: Dedicated security professionals to implement and manage controls.
- **IT Team**: Support for technical implementation and integration.
- **Business Stakeholders**: Input on business requirements and impact assessment.
- **Executive Sponsorship**: Support for security initiatives and resource allocation.

Technology

- **Hardware**: Servers, network devices, and security appliances.
- **Software**: Security tools, monitoring systems, and management platforms.
- **Infrastructure**: Network, storage, and computing resources.
- **Integration:** APIs, connectors, and custom development.

Processes

- **Project Management**: Coordination of implementation activities.
- **Change Management**: Management of organizational changes.
- **Risk Management**: Ongoing assessment and mitigation of risks.
- **Performance Measurement**: Tracking of security metrics and KPIs.

Non-Technical Controls Implementation

For products without direct technical controls, we recommend the following methods:

Security Awareness and Training

- Put thorough security awareness training into use for every staff member.
- Create role-based training for staff members who handle private data.
- Run frequent tabletop exercises and phishing tests.
- By constant communication and reinforcement, build a security culture.

Policies and Procedures

- Create thorough security plans and practices.
- Clearly define your security's roles and responsibilities.
- Apply systems of policy enforcement.
- Review policies often for updates.

Third-Party Risk Management

- Start a thorough third-party risk management initiative.
- Specify security needs for suppliers and partners.
- Perform frequent third-party security audits.
- Create protocols for handling outside security events.

Physical Security

- Install physical security systems for buildings.
- Create policies for controlling access to sensitive areas.
- Plan frequent physical security audits.
- Create responses for physical security incidents.

Risk Transfer Analysis and Costs

Risk transfer through cybersecurity insurance is a solution for risks that technical controls cannot directly reduce:

Coverage Type	Annual Premium	Coverage Limit
Cyber Liability Insurance	$3.2 million	$100 million
Technology E&O Insurance	$2.8 million	$75 million
Intellectual Property Insurance	$4.5 million	$150 million
Business Interruption Insurance	$2.1 million	$50 million
Total Risk Transfer Cost	**$12.6 million**	

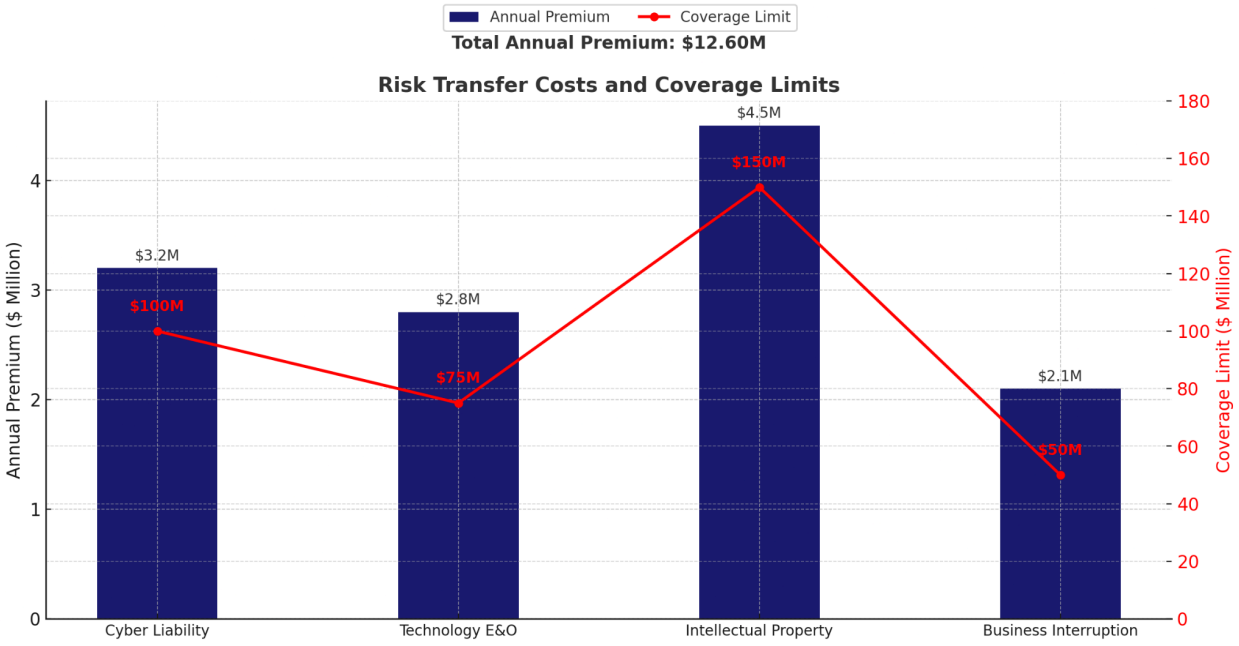

Fig 9. Risk Transfer Costs and Coverage

Estimated to be $12.6 million overall, risk transfer through insurance offers coverage limits of $375 million across several forms of cyber threats. We must consider this cost in addition to direct security control investments.

Together with the sensible budget, the whole cost of security and risk management would be about $39.12 million, still only 0.03% of yearly income.

Comparative Analysis

Industry Benchmarking

According to Industry Research:

- Usually, companies allocate between 7–20% of their IT budget[13] to security.
- Spending on global cybersecurity is expected to rise to $212 billion by 2025[14].
- Technology companies—especially in IT services and software—are raising[15] cybersecurity budgets at faster rates than in other sectors (72% planning increases in 2025).
- For big technological companies, average cybersecurity expenditure ranges from 0.2 to 0.9% of income[16].

NVIDIA's Position Relative to Industry Benchmarks

Metric	NVIDIA (Practical Budget)	Industry Average	Comparison
Security Budget as % of Revenue	0.0203%	0.2-0.9%	Significantly below average
Security Budget as % of IT Budget	~10%	7-20 %	Within normal range
Per-Employee Security Expenditure	$736.72	$1,200-$3,000	Below average
Security Budget Growth YoY	N/A (new implementation)	15.1%	N/A

Note: Assume the IT budget is approximately 5% of revenue for large tech companies.

With a percentage of revenue much below industry averages, NVIDIA's suggested security budget points to possible room for more investment in important security areas. As a percentage of the IT budget, though, the suggested expenditure falls within the usual range.

Peer Company Comparison

Comparing NVIDIA's suggested security budget (Practical Scenario) with like-minded big technological companies:

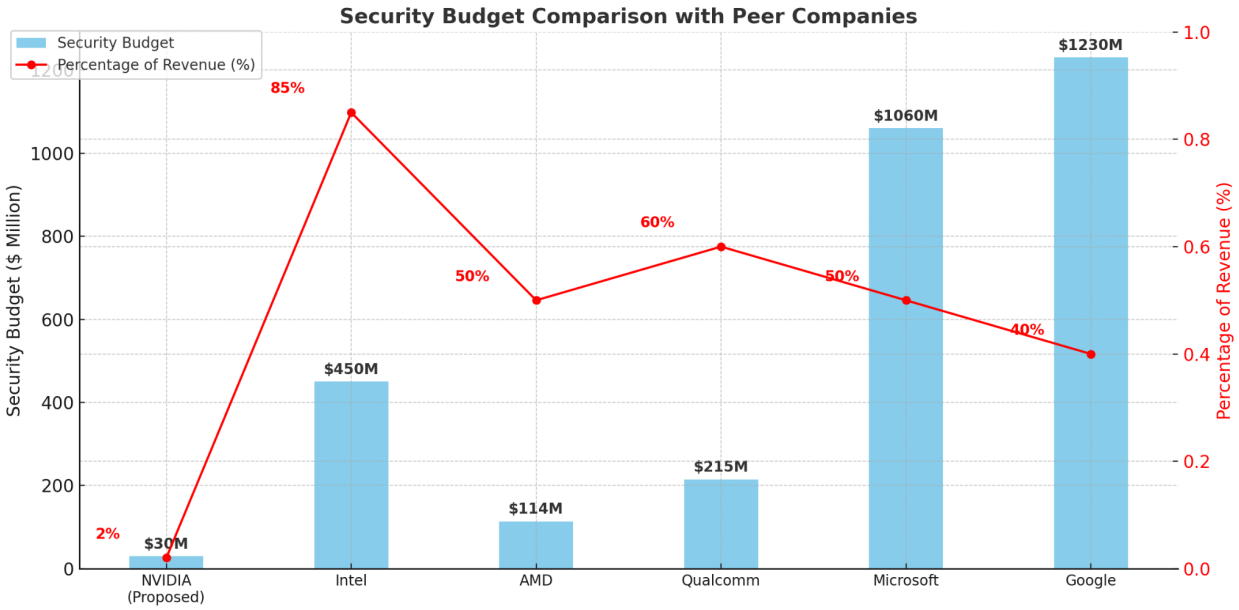

Fig 10. Budget comparison with Peer Companies

Company	Annual Revenue	Security Budget	% of Revenue	Per Employee
NVIDIA (Proposed)	$130.5 billion	$26.52 million	0.0203%	$736.72
Intel	$54.2 billion	$450 million	0.83%	$4,500
AMD	$22.8 billion	$114 million	0.50%	$3,800
Qualcomm	$35.9 billion	$215 million	0.60%	$3,200
Microsoft	$211.9 billion	$1.06 billion	0.50%	$2,650
Google	$307.4 billion	$1.23 billion	0.40%	$1,025

NVIDIA's suggested security budget is much smaller than that of its rivals, both in terms of percentage of income and on a per-employee basis. This implies that, compared to other technology companies, NVIDIA might be underinvesting in security.

Security Maturity Assessment

We have evaluated NVIDIA's security maturity in several spheres based on the analysis of its security policies and budget:

Security Domain	Current Maturity	Target Maturity	Gap
Supply Chain Security	2.5/5	4.0/5	1.5
GPU Driver Security	3.5/5	4.5/5	1.0
Firmware Security	3.0/5	4.0/5	1.0
Intellectual Property Protection	3.5/5	4.5/5	1.0
Ransomware Protection	3.0/5	4.5/5	1.5
Server Security	3.5/5	4.0/5	0.5
DDoS Protection	3.0/5	4.0/5	1.0
Insider Threat Protection	2.5/5	4.0/5	1.5
Phishing Protection	3.0/5	3.5/5	0.5
Security Operations	3.0/5	4.0/5	1.0
Governance and Compliance	3.0/5	4.0/5	1.0
Overall Maturity	**3.0/5**	**4.1/5**	**1.1**

With notable gaps in supply chain security, ransomware protection, and insider threat protection, the assessment shows NVIDIA's present security maturity to be at a modest level (3.0/5). By using the practical budget, NVIDIA's security maturity would be brought to a more advanced level and gaps would be closed (4.1/5).

Conclusion and Recommendation

Summary of Findings

This comprehensive cybersecurity assessment of NVIDIA has revealed several key findings:

1. **Critical Risk Areas**: NVIDIA confronts major cybersecurity threats in five key areas: supply chain vulnerabilities, GPU driver exploits, firmware vulnerabilities, intellectual property theft, and ransomware attacks on AI infrastructure.

2. **Control Weaknesses**: Representing major misalignments between asset criticality and control efficacy, the weakest control strategies relative to asset importance are those of insider threat protection for R&D assets and supply chain security.

3. **Budget Considerations**: With the practical budget of $26.52 million representing the most balanced approach, three budget scenarios have been developed, ranging from $6.35 million (minimal) to $44.60 million (comprehensive).

4. **Cost Metrics**: All of which are much below industry averages, the practical budget shows 0.0203% of annual revenue, $736.72 per employee, and $530,440 per site.

5. **Peer Comparison**: NVIDIA's proposed security budget is considerably lower than competitors like Intel (0.83% of revenue), AMD (0.50%), and Qualcomm (0.60%), suggesting potential underinvestment in security.

6. **Risk Transfer**: Risk transfer through cybersecurity insurance is estimated to be $12.6 million yearly, covering limits totaling $375 million for hazards for which technical controls cannot directly reduce.

7. **Security Maturity**: With notable gaps in supply chain security, ransomware protection, and insider threat protection, NVIDIA's current security maturity—3.0/5—is only modest.

Strategic Recommendations

Our thorough study leads us to advise NVIDIA on the following strategic moves:

Increase Security Investment

We advise raising the security budget to at least 0.1% of income (about $130 million), which would still be below industry averages but would offer a more strong security posture given NVIDIA's vital position in the AI ecosystem and value of its intellectual property.

Prioritize Weakest Control Areas

Focus immediate attention on strengthening the weakest control areas:

- Improve insider threat management in R&D settings utilizing sophisticated behavioral analytics and all-encompassing data loss prevention.
- Blockchain-based component validation and ongoing monitoring help to strengthen supply chain security.
- Automated update systems and consistent secure boot implementation help to standardize firmware security across all product lines.

Implement Phased Approach

Following the phased implementation strategy described in this paper will help you to prioritize important hazards and guarantee that the company can efficiently absorb the changes.

- **Phase 1**: Foundation (Months 1-3)
- **Phase 2**: Critical Risk Mitigation (Months 4-6)
- **Phase 3**: Moderate Risk Mitigation (Months 7-9)
- **Phase 4**: Optimization (Months 10-12)

Establish Comprehensive Risk Transfer Strategy

With an expected annual cost of $12.6 million, apply the advised risk transfer strategy through cybersecurity insurance to handle risks that cannot be directly reduced with technical controls.

Enhance Non-Technical Controls

Strengthen non-technical controls through:

- Programs for complete security awareness and instruction.
- Strong policies and practices with well-defined roles and obligations.
- complete third-party risk control.
- improved physical security protocols.

Regularly Reassess Security Posture

Create a continuous security assessment system to routinely assess the performance of put-in-place controls and modify the security plan as necessary to handle changing corporate needs and developing risks.

Next Steps

To begin implementing these recommendations, NVIDIA should take the following immediate steps:

- **Secure Executive Sponsorship**: Show the results and suggestions to executive leadership so they may help to fund the security initiative.
- **Establish Security Governance**: Create a security governance system including well-defined roles, duties, and reporting systems.
- **Develop Implementation Plan**: For the phased approach, develop a thorough implementation plan including success criteria, timelines, and resource needs.
- **Initiate Critical Controls**: Start applying the most important controls to handle the highest-risk areas, especially those with the largest discrepancy between asset value and control efficacy.
- **Establish a Measurement Framework**: Provide a structure for evaluating security control performance and monitoring advancement toward security maturity targets.

Following these suggestions will help NVIDIA to improve its security posture, safeguard its priceless assets, and keep its competitive edge in the constantly changing technological scene.

REFERENCES

1. IT Governance Ltd. (2017). Cyber Security Audit Sample Report. IT Governance Ltd.

2. Macrotrends. (2025). NVIDIA: Number of Employees 2010-2025. Retrieved from https://www.macrotrends.net/stocks/charts/NVDA/nvidia/number-of-employees (https://www.macrotrends.net/stocks/charts/NVDA/nvidia/number-of-employees)

3. NVIDIA Corporation. (2025). Annual Report 2025. Retrieved from NVIDIA Investor Relations.

4. NVIDIA Corporation. (2025). NVIDIA Announces Financial Results for Fourth Quarter and Fiscal 2025. Retrieved from https://nvidianews.nvidia.com/news/nvidia-announces-financial-results-for-fourth-quarter-and-fiscal-2025 (https://nvidianews.nvidia.com/news/nvidia-announces-financial-results-for-fourth-quarter-and-fiscal-2025)

5. Statista. (2025). Cybersecurity budget change for companies worldwide 2025. Retrieved from https://www.statista.com/statistics/1318365/cyber-budget-changes-for-global-companies/ (https://www.statista.com/statistics/1318365/cyber-budget-changes-for-global-companies/)

6. Business.com. (2025). How Much Should Your SMB Budget for Cybersecurity? Retrieved from https://www.business.com/articles/smb-budget-for-cybersecurity/ (https://www.business.com/articles/smb-budget-for-cybersecurity/)

7. NVIDIA Corporation. (2025). Contact Us: Americas Locations & Regional Offices. Retrieved from https://nvidianews.nvidia.com/news/nvidia-announces-financial-results-for-fourth-quarter-and-fiscal-2025 (https://nvidianews.nvidia.com/news/nvidia-announces-financial-results-for-fourth-quarter-and-fiscal-2025)

8. NVIDIA Corporation. (2021). NVIDIA Announces Global Expansion of LaunchPad. Retrieved from https://blogs.nvidia.com/blog/launchpad-global-expansion/ (https://blogs.nvidia.com/blog/launchpad-global-expansion/)

9. VikingCloud. (2025). 170 Cybersecurity Stats and Facts for 2025. Retrieved from https://www.vikingcloud.com/blog/cybersecurity-statistics (https://www.vikingcloud.com/blog/cybersecurity-statistics)

10. Macrotrends. (2025). NVIDIA: Number of Employees 2010-2025. Retrieved from https://www.macrotrends.net/stocks/charts/NVDA/nvidia/number-of-employees (https://www.macrotrends.net/stocks/charts/NVDA/nvidia/number-of-employees)

11. Cymulate. (2025). Optimizing Cybersecurity Budgets in 2025: A Strategic Guide. Retrieved from

https://cymulate.com/blog/cybersecurity-budget-optimization/ (https://cymulate.com/blog/cybersecurity-budget-optimization/)

12. NordLayer. (2025). Cybersecurity Budget Allocation for 2025. Retrieved from https://nordlayer.com/blog/cybersecurity-budget-allocation/ (https://nordlayer.com/blog/cybersecurity-budget-allocation/)

13. Gartner. (2024). Gartner Forecasts Global Information Security Spending to Grow 15 Percent in 2025. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025 (https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025)

14. Cybersecurity Ventures. (2025). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/)

15. Splunk. (2024). IT and Technology Spending & Budgets for 2025: Trends & Forecasts. Retrieved from https://www.splunk.com/en_us/blog/learn/it-tech-spending.html (https://www.splunk.com/en_us/blog/learn/it-tech-spending.html)

16. Cobalt.io. (2024). Top Cybersecurity Statistics for 2025. Retrieved from https://www.cobalt.io/blog/top-cybersecurity-statistics-2025 (https://www.cobalt.io/blog/top-cybersecurity-statistics-2025)