Organizational Cybersecurity Evaluation

Part 3

NVIDIA SECURITY CONTROLS ASSESSMENT

Prepared by: Shriram Karpoora Sundara Pandian

TABLE OF CONTENTS

Executive Summary

This report presents a comprehensive assessment of security controls designed to mitigate the vulnerabilities and risks identified in the previous NVIDIA risk assessment. The analysis builds upon the findings of the vulnerability and risk assessment conducted in Part 2, which identified several critical, moderate, and low-risk areas that could potentially impact NVIDIA's operations, intellectual property, and infrastructure.

Key Findings

The risk assessment done previously on part 2 identified nine primary vulnerabilities or risks affecting NVIDIA with different levels of probability and impact. After careful consideration, supply chain vulnerability, GPU driver exploits, firmware vulnerabilities, intellectual property theft, and ransomware attacks on NVIDIA's AI infrastructure are the critical risks. As they are crucial to mitigate, we need to place the necessary controls, take robust measures, and reduce the probability of it negatively impacting the operations and reputation of the company.

Security Control Framework

For the risk identified, the report provides different security control options, which can be categorized into four types:

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

Each control has been evaluated for its relative cost and effectiveness, with particular attention to how well it addresses the specific risk factors identified in the probability versus impact matrix from Part 2.

Prioritized Recommendations

These top-ranked security controls prioritize mitigating critical risks with high effectiveness measures:

- **Supply Chain Security**: Deploying thorough vendor review programs, ongoing oversight of supply chain processes, and part processes to validate operations and control vulnerabilities in the supply chain.
- **GPU Driver Security**: Automated driver update management, driver whitelisting, and real-time driver activity monitoring capabilities to stop and identify GPU driver exploits.
- **Firmware Protection**: Automating firmware update management, firmware validation procedures, and secure boot implementations to mitigate firmware vulnerabilities.

- **Intellectual Property Protection**: NVIDIA's Confidential Computing to Protect Your Intellectual Property on H100 GPUs, which limits access and encrypts data to safeguard against intellectual property theft.
- **Ransomware Defense:** Deploying AI-Enhanced Security [1] Using NVIDIA BlueField DPUs and the Morpheus cybersecurity framework [2]. Providing integrated ransomware defense using backups and network segmentation attacks.

Implementation Considerations

These security controls must be implemented in a risk-based manner, maximizing effectiveness to cost by focusing on high critical risks. Organizations should evaluate their unique setting, current security architecture, and asset limitations to determine which controls to implement.

This report will serve as a guide on how to improve NVIDIA's security posture by adding a new protective layer that considers the entire range of identified risks. Implementing these recommended security controls will greatly decrease the attack surface of NVIDIA, its vulnerability to cyber threats and its capability of securing its products and operations.

Introduction

Purpose and Scope

This report frequently refers to the vulnerability and risk assessment discussed in Part 2 for NVIDIA Corporation. This document serves as a way to create a full list of security controls capable of effectively addressing the vulnerabilities and risks identified earlier. After listing for each vulnerability/risk pair a set of multiple control options, which are giving a wide spectrum of options for NVIDIA to improve their security defense.

This assessment covers:

- In-depth analysis for every vulnerability and risk highlighted in Part 2.
- Creation of several security control alternatives for each vulnerability/risk combination.
- Type categorization of the controls (Detective, Preventative, Forensic, Audit).
- Approximate costs for each control.
- Hierarchy of controls (ranked by effectiveness) aligned to the likelihood vs impact matrix from Part 2.

It will also use this assessment to make recommendations that NVIDIA can use to ensure that cybersecurity practices can be enforced on their end to avoid these threats and secure their critical assets, intellectual property, and infrastructure.

Methodology

My goal is to cover all the parts of NVIDIA's infrastructure so that we can cover the whole attack surface and address the risks associated with it.

1. **Risk Analysis**: We will analyze the vulnerabilities and risks that we found in part 2 and try to address them better.
2. **Control Identification**: It is better to have more controls to reduce the risk to form the defense in depth, so we tried to find more controls through research and NVIDIA security frameworks and documentation.
3. **Control Categorization**: Before establishing the control, as a rule of thumb, we already categorized them, which I have mentioned at the top of the report. It will help us to understand the controls better and implement them effectively.
4. **Cost Estimation**: There is always a budget for everything in an enterprise, so we need to find an optimal cost solution for implementing this control, so rank them based on the relative cost (low, medium, and high) and its requirements.
5. **Effectiveness Ranking**: We will rank the controls and their effectiveness in addressing the critical risks based on the probability and impact ratings from Part 2.
6. **Prioritization**: In this part, we will combine everything—effectiveness, cost, and ease of implementation—into consideration and do accordingly.

By following this methodology, we can provide better controls and value to NVIDIA's specific risks and vulnerabilities. It will help to build a robust infrastructure as a whole.

Before diving deep into the controls, just a brief overview of the risk we identified and a mention of the matrix table so it will be easier to understand the controls specified.

Risk and Vulnerability Assessment Summary

Overview of Identified Risks

As NVIDIA is a matured organization now, the risks we identified in part 2 were based on the publicly available resource; there is no active pentesting involved, but there are a total of 9 vulnerability/risk pairs identified that can cover all parts of the organization and help us better address those threats that can arise. The following risk may vary in both probability of occurrence and potential impact, requiring a tailored approach to security controls.

The key risks identified include:

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 the insider threats that could compromise NVIDIA's research and architectures, including some 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.

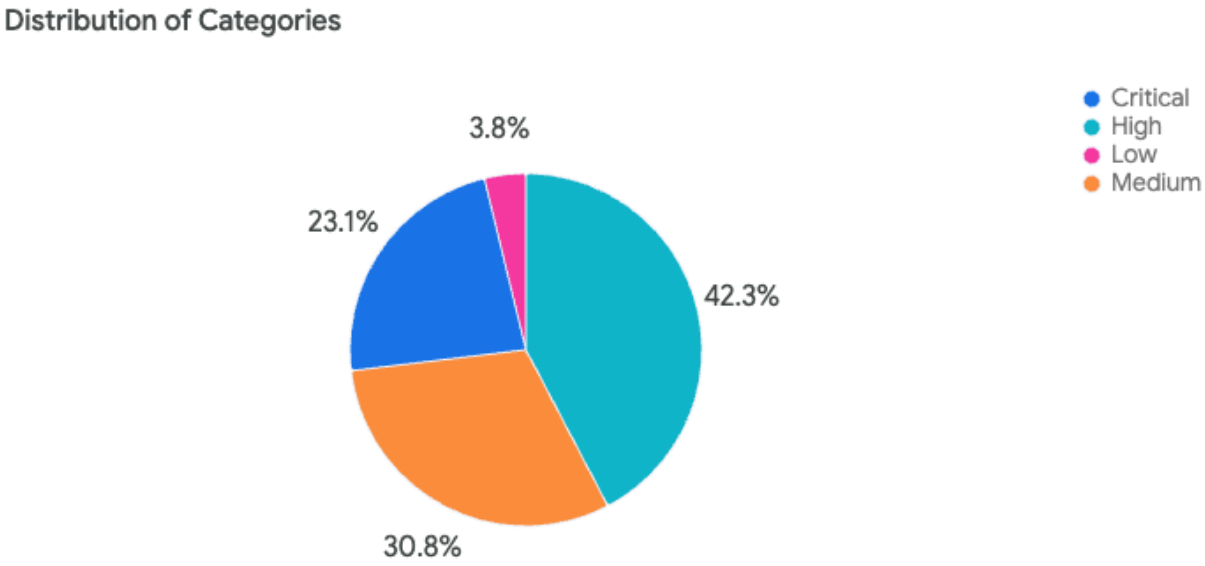
Probability vs. Impact Matrix

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 semiconductor manufacturing	Medium	High	Critical
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.



With regard to both the probability of occurrence and the possible influence, the security controls offered in the following sections are meant to handle these particular risks. Based on their ability to reduce the found hazards, controls are ranked; special focus is on those addressing important risks.

Security Controls by Risk Category

We will address security controls and break them down one by one based on the risk category that we identified and discussed on document 2. We will categorize them by type (Preventative, Detective, Forensic, and Audit) and finally include relative cost estimates.

Supply Chain Vulnerabilities

RSA events are addressing this vulnerability, which is a huge attack vector, and managing them effectively is the topmost priority for product-based and B2B companies that deal with supplies and vendors, retailers, and finally, customers. As important as it sounds, we need to address it for NVIDIA as well [4]. This is due to their status as global players in the industry.

Preventative Controls

1.1 Vendor Assessment and Due Diligence

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

Implementation

- 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 [5] ISO 27001, NIST [6] and SOC 2, etc.
- Conduct on-site security assessments for critical suppliers.

Relative Cost: Medium-High
Control Type: Preventative

1.2 Supply Chain Visibility

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

Implementation

- 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.

Relative Cost: Medium
Control Type: Preventative

1.3 Secure-by-Design Approach

Increasing the robustness of the products, such as firmware and driver updates from the code level, involves integrating software testing tools and ensuring security requirements from the product design phase to the final output.

Implementation

- Implement security requirements in the product design phase.
- As mentioned above, use secure coding practices for all development.
- Perform threat modeling during the design phase.
- Conduct regular security reviews at key development milestones.

Relative Cost: Medium-High
Control Type: Preventative

1.4 Component Validation

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

Implementation

- 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.

Relative Cost: Medium
Control Type: Preventative

Detective Controls

1.5 Continuous Monitoring

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

Implementation

- Use AI-based [7] (reinforcement-based) anomaly detection for supply chain operations.

- Monitor for unauthorized access or changes to components.
- Establishing an SOC (security operations center) for supply chain.

Relative Cost: High
Control Type: Detective

1.6 Vulnerability Scanning

Scan third-party libraries, dependencies, and modules for known vulnerabilities regularly.

Implementation

- Regularly scan third-party components for vulnerabilities.
- Implementation of automated scanning in the CI/CD pipeline.
- Having regular feeds to vulnerability feeds for third-party components.

Relative Cost: Medium
Control Type: Detective

Forensic Controls

1.7 Incident Response Planning

Develop specific incident response procedures and planning for supply chain security incidents.

Implementation

- Creating in-depth procedures for supply chain-specific incident response.
- Enabling evidence-gathering software like FTK and Encase to increase the forensic capability of supply chain incidents.
- Putting the evidence collection protocols.
- Conduct regular tabletop exercises for supply chain incidents.

Relative Cost: Medium
Control Type: Forensic

Audit Controls

1.8 Regular Audits

Continuously auditing and reviewing the suppliers and their security practices and protocols.

Implementation

- Conduct periodic audits of suppliers and their security practices.
- Perform compliance checks regularly against industry standards.
- Verify the implementation of security controls.
- Document and track remediation of audit findings.

Relative Cost: Medium-High
Control Type: Audit

1.9 Supply Chain Security Metrics

Establish and track key performance indicators for supply chain security.

Implementation

- Establish KPIs for supply chain security.
- Track and report on security incidents related to the supply chain.
- Measure the effectiveness of controls.
- Regularly review and update metrics.

Relative Cost: Low-Medium
Control Type: Audit

GPU Driver Exploits

For NVIDIA, GPU driver exploits pose a serious threat [8] 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.

Preventative Controls

2.1 Regular Driver Updates

Maintain an effective patch management program for GPU drivers.

Implementation

- 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.

Relative Cost: Medium
Control Type: Preventative

2.2 Driver Whitelisting

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

Implementation

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

Relative Cost: Medium
Control Type: Preventative

2.3 Secure Boot Process

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

Implementation

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

Relative Cost: Medium
Control Type: Preventative

2.4 Secure Driver Installation Process

Provide a safe system for driver installation to stop illegal changes.

Implementation

- Install drivers from reliable sources just once.
- Check driving package digital signatures.
- Install driver access control based on roles.
- Log all of the driver installation events.

Relative Cost: Low-Medium
Control Type: Preventative

Detective Controls

2.5 Driver Activity Monitoring

Track driver behavior to find possible security problems.

Implementation

- 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.

Relative Cost: Medium-High
Control Type: Detective

2.6 Vulnerability Scanning

Check for known driver vulnerabilities often.

Implementation

- Scan often for known [9] driver vulnerabilities.
- Subscribe to GPU driver security advice.
- Put automated scanning tools into use.
- Sort weaknesses in order of risk.

Relative Cost: Medium
Control Type: Detective

Forensic Controls

2.7 Incident Response

Provide particular incident response protocols for security events involving drivers.

Implementation

- Create incident response protocols tailored to driver exploits.
- Provide forensic capability for events involving drivers.
- Establish procedures for gathering evidence.
- Plan frequent tabletop exercises for driver exploit scenarios.

Relative Cost: Medium
Control Type: Forensic

Audit Controls

2.8 Driver Configuration Audits

Check driver configurations often to guarantee security policy compliance.

Implementation

- Review and audit driver configurations regularly.
- Check security policy compliance.
- List all installed versions and drivers.
- Track and fix audit result findings.

Relative Cost: Low-Medium
Control Type: Audit

Firmware Vulnerabilities

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.

Preventative Controls

3.1 Regular Firmware Updates

Keep up a good firmware patch management [10] schedule.

Implementation

- 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.

Relative Cost: Medium
Control Type: Preventative

3.2 Firmware Validation

Verify before installation the integrity and authenticity of firmware updates.

Implementation

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

Relative Cost: Medium
Control Type: Preventative

3.3 Secure Boot

Use Safe Boot to confirm firmware integrity during system start.

Implementation

- Put Secure Boot on NVIDIA GPUs in effect.
- Load only authorized firmware during boot.
- Manage safe boot choices in BIOS/UEFI.
- Put boot integrity verification into effect.

Relative Cost: Medium
Control Type: Preventative

3.4 Secure Communication Protocols

Update firmware using safe communication channels.

- Update firmware using SSH or HTTPS.
- Encrypt programs for firmware updates.
- Put in place safe firmware updating channels.
- Check the mechanisms of update distribution security.

Relative Cost: Medium
Control Type: Preventative

Detective Controls

3.5 Firmware Update Activity Monitoring

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.

Relative Cost: Medium
Control Type: Detective

3.6 Vulnerability Scanning

Search for known firmware flaws often.

- Search often for known firmware flaws.
- Subscribe to GPU firmware security advice.
- Put automated scanning tools into use.
- Sort weaknesses in order of risk.

Relative Cost: Medium
Control Type: Detective

Forensic Controls

3.7 Incident Response

Provide particular incident response protocols for security events involving firmware.

- Create incident response protocols tailored for a given firmware platform.
- Provide forensic capability for events involving firmware.
- Establish procedures for gathering evidence.
- Perform frequent tabletop exercises covering firmware exploit situations.

Relative Cost: Medium
Control Type: Forensic

Audit Controls

3.8 Firmware Configuration Audits

Frequent firmware configuration audits help ensure security policy compliance.

- Review and audit firmware regularly.
- Verify security policy compliance.
- Record every firmware update.
- Track and fix audit result findings.

Relative Cost: Low-Medium
Control Type: Audit

Intellectual Property Theft and Industrial Espionage

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.

Preventative Controls

4.1 Confidential Computing

Use NVIDIA's Confidential Computing [11] 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.

Relative Cost: High
Control Type: Preventative

4.2 Access Control

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.

Relative Cost: Medium
Control Type: Preventative

4.3 Data Encryption

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.

Relative Cost: Medium-High
Control Type: Preventative

4.4 DLP Solutions

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

- Using tools for data loss prevention.
- Track and regulate data exchanges.
- Block illegal data leaks.
- Use content inspection on sensitive information.

Relative Cost: High
Control Type: Preventative

Detective Controls

4.5 User Behaviour Analytics

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.

Relative Cost: High
Control Type: Detective

4.5 Network Monitoring

Track network traffic looking for possible data exfiltration.

- Track network traffic looking for data exfiltration.
- Use deep packet checking.
- Detect anomalies using artificial intelligence.
- Track for odd data movement trends.

Relative Cost: High
Control Type: Detective

Forensic Controls

4.7 Incident Response

Provide particular incident response protocols for cases of intellectual property theft.

- Create incident responses tailored for IP theft.
- Provide forensic capacity for events involving IP theft.
- Establish procedures for gathering proof.
- Plan frequent tabletop exercises for IP theft scenarios.

Relative Cost: Medium-High
Control Type: Forensic

4.8 Digital Forensics

Keep yourself forensic ready for investigations on intellectual property theft.

- Keep yourself forensically ready for investigations on IP theft.

- Put instruments for gathering digital evidence into use.
- Create chains of custody policies.
- Staff should be taught forensic techniques.

Relative Cost: High
Control Type: Forensic

Audit Controls

4.9 Access Audits

Check access to sensitive intellectual property often.

- Routinely check sensitive IP access.
- Review access logs and rights.
- Check security policy compliance.
- Track and fix results from audits.

Relative Cost: Medium
Control Type: Audit

4.10 Security Awareness Training

Provide regular security awareness courses with an eye toward intellectual property protection.

- Provide frequent IP protection instruction.
- Teach staff members security policies.
- Simulate attacks to gauge awareness.
- Calculate the degree of training success.

Relative Cost: Medium
Control Type: Audit

Ransomware Attacks on NVIDIA’s AI Infrastructure

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.

Preventative Controls

5.1 AI-Enhanced Security

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.

Relative Cost: High
Control Type: Preventative

5.2 Network Segmentation

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.

Relative Cost: High
Control Type: Preventative

5.3 Backup and Recovery

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.

Relative Cost: Medium-High
Control Type: Preventative

5.4 Endpoint Detection

Apply sophisticated endpoint security to stop ransomware from spreading.

- Install next-generation antivirus programs.
- Use whitelisting in applications.
- Apply behavior-based malware identification.
- Install endpoint detection and response (EDR) tools.

Relative Cost: Medium
Control Type: Preventative

Detective Controls

5.5 Behavioral Monitoring

Track for 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.

Relative Cost: Medium
Control Type: Preventative

5.6 Threat Intelligence

Use threat intelligence to remain current with ransomware concerns.

- Get threat intelligence feeds subscribed to.
- Watch for signals of compromise.
- Put automated threat detection into action.
- Share intelligence on threats with business partners.

Relative Cost: Medium
Control Type: Detective

Forensic Controls

5.7 Incident Response

Establish specific protocols for ransomware events.

- Create incident response protocols tailored especially for ransomware.
- Provide forensics for ransomware events.
- Design procedures for gathering evidence.
- Plan frequent tabletop exercises for ransomware scenarios.

Relative Cost: Medium-High
Control Type: Forensic

5.8 Digital Forensics

Maintain forensic preparedness for any investigations on ransomware.

- Keep forensics prepared to begin investigations on ransomware.
- Put instruments for gathering digital evidence into use.
- Create chains of custody policies.
- Staff should be taught forensic techniques.

Relative Cost: High
Control Type: Forensic

Audit Controls

5.9 Security Posture Assessment

Compare security posture often with ransomware risks.

- Review security posture often in relation to ransomware.
- Perform penetration tests.
- Check vulnerabilities.
- Conducting a simulation of ransomware attacks.

Relative Cost: Medium-High
Control Type: Audit

5.10 Security Awareness Training

Plan frequent security awareness campaigns with an eye toward ransomware avoidance.

- Provide frequent ransomware prevention instruction.
- Teach staff members security policies.
- Simulate attacks to gauge awareness.
- Calculate the degree of training success.

Relative Cost: Medium
Control Type: Audit

Server Vulnerabilities

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

Preventative Controls

6.1 Patch Management

Place 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.

Relative Cost: Medium
Control Type: Preventative

6.2 Secure Configuration

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.

Relative Cost: Medium
Control Type: Preventative

6.3 Application Security

Include application security to guard servers.

- Apply safe coding methods.
- Review codes here.
- Test application security both dynamically and statistically.
- Put web application firewalls into use.

Relative Cost: Medium-High
Control Type: Preventative

6.4 Network Security

Install network security systems to guard servers.

- Use IPS/IDS and firewalls.
- Include the principle of least privilege for network access.
- Segmentation of networks.
- Set network access limits.

Relative Cost: Medium-High
Control Type: Preventative

Detective Controls

6.5 Vulnerability Scanning

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

Relative Cost: Medium
Control Type: Detective
6.6 Log Monitoring

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.

Relative Cost: High
Control Type: Detective

Forensic Controls

6.7 Incident Response

Create particular incident response protocols for security events pertaining to servers.

- Establish incident response plans tailored for server vulnerabilities.
- Develop the forensic capacity for events involving servers.
- Provide procedures for gathering evidence.
- Plan frequent tabletop exercises for scenarios involving server compromise.

Relative Cost: Medium
Control Type: Forensic

Audit Controls

6.8 Configuration Audits

Regular server configuration audits help ensure security policy compliance.

- Frequent audits of server configurations
- Check compliance with security guidelines.
- Record every configuration for a server.
- Track and fix audit result findings.

Relative Cost: Medium
Control Type: Audit

6.9 Penetration Testing

Investigate server vulnerabilities often through penetration testing.

- Perform consistent penetration testing.
- Simulate strikes to find weaknesses.
- Act right away based on findings.
- Check the efficiency of remedial action.

Relative Cost: High
Control Type: Audit

DDoS Attacks on NVIDIA Cloud Services

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

Preventative Controls

7.1 Traffic Management

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.

Relative Cost: Medium-High
Control Type: Preventative

7.2 Deep Learning-based DDoS Protection

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

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

Relative Cost: High
Control Type: Preventative

7.3 Rate Limiting

Put rate limiting into use to stop resource depletion.

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

Relative Cost: Medium
Control Type: Preventative

7.4 CDN Services

DDoS traffic can be absorbed with content delivery networks.

- Apply Content Distribution Networks
- Evenly distribute traffic among several servers.
- Process DDoS attacks.
- Put anycast routing into effect.

Relative Cost: Medium-High
Control Type: Preventative

Detective Controls

7.5 Traffic Analysis

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.

Relative Cost: Medium-High
Control Type: Detective

7.6 DDoS Detection Systems

Install specialized DDoS detection systems.

- Set up specialized DDoS-detecting mechanisms.
- Set off alarms for dubious traffic.
- Combine with systems of mitigation.
- Put real-time monitoring into effect.

Relative Cost: High
Control Type: Detective

Forensic Controls

7.7 Incident Response

Create particular protocols for DDoS attacks.

- Establish incident response systems tailored for DDoS attacks.
- Provide DDoS incident forensic capabilities.
- Establish procedures for gathering proof.
- Create frequent tabletop exercises for DDoS scenarios.

Relative Cost: Medium
Control Type: Forensic

Audit Controls

7.8 DDoS Readiness Assessment

Routinely evaluate DDoS preparedness.

- Evaluate DDoS preparedness often.
- Perform virtual DDoS assaults.
- Examine and change mitigating plans.
- Test DDoS reaction protocols.

Relative Cost: Medium-High
Control Type: Audit

Insider Threats Affecting R&D

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 [12].

Preventative Controls

8.1 Access Control

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.

Relative Cost: Medium
Control Type: Preventative

8.2 Data Loss Prevention

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.

Relative Cost: High
Control Type: Preventative

8.3 Physical Security

Install physical security systems to guard R&D buildings.

- Place access control mechanisms.
- Employ video surveillance.
- Safe in-person documentation
- Set up safe spaces for delicate work.

Relative Cost: Medium-High
Control Type: Preventative

8.4 Security Awareness Training

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.

Relative Cost: Medium
Control Type: Preventative

Detective Controls

8.5 User Behavior Analytics

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.

Relative Cost: High
Control Type: Detective

8.6 Log Monitoring

Track logs for unusual behavior suggesting insider threats.

- Standardize and track access records.
- Adopt SIEM solutions.
- AI for log analysis
- Set up alarms for odd behavior.

Relative Cost: High
Control Type: Detective

Forensic Controls

8.7 Incident Response

Create customized incident response protocols for insider threat events.

- Develop incident response policies tailored for insider threats.
- Build forensic capacity for events involving insider threats.
- Establish procedures for gathering evidence.
- Frequent tabletop exercises for insider threat scenarios.

Relative Cost: Medium
Control Type: Forensic

8.8 Digital Forensics

Keep yourself forensic ready for investigations on insider threats.

- Maintain forensic readiness for investigations on insider threats.
- Put instruments for gathering digital evidence into use.
- Create chains of custody policies.
- Staff should be taught forensic techniques.

Relative Cost: High
Control Type: Forensic

Audit Controls

8.9 Access Audits

Audit sensitive system access on a regular basis.

- Regularly check sensitive system access.
- Examine permissions and access logs.
- Check security policy compliance.
- Track and fix results from audits.

Relative Cost: Medium
Control Type: Audit

8.10 Background Checks

Investigate employees who have access to sensitive data carefully.

- Perform extensive staff background checks.
- Re-screen on a regular basis.
- Verify references and qualifications.
- Use ongoing assessment for highly risk-bearing roles.

Relative Cost: Medium
Control Type: Audit

Phishing Attacks Leading to Credential Theft

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.

Preventative Controls

9.1 AI-Enhanced Email Security

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

- Use NVIDIA Morpheus [13] to spot spear phishing [14].
- Find phishing attempts using generative artificial intelligence.
- Install email filtering tools.
- Put URL and attachment scanning into action.

Relative Cost: High
Control Type: Preventative

9.2 Multi-Factor Authentication

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.

Relative Cost: Medium
Control Type: Preventative

9.3 Security Awareness Training

Provide regular security awareness courses with an eye toward phishing avoidance [15].

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

Relative Cost: Medium
Control Type: Preventative

9.4 Email Authentication

Utilize email authentication methods to stop email spoofing.

- Using SPF, DKIM, and DMARC:
- Set email gates to filter phony messages.
- Leverage email authentication systems.
- Track instances of email authentication failing.

Relative Cost: Low-Medium
Control Type: Preventative

Detective Controls

9.5 Email Monitoring

Track email traffic in search of possible phishing efforts.

- Monitor for suspicious email trends [16].
- Put URL and attachment scanning into use.
- Analyze emails using artificial intelligence.
- Create alerts in case of possible phishing efforts.

Relative Cost: Medium-High
Control Type: Detective

9.6 User Behavior Analytics

Track unusual login behavior that might point to credential theft.

- Monitor unusual login trends.
- Search for signs of credential theft.
- Track account use.
- Create benchmarks for regularity of behavior.

Relative Cost: High
Control Type: Detective

Forensic Controls

9.7 Incident Response

Create customized incident response protocols for phishing events.

- Develop incident response systems tailored for phishing.
- Build forensic skills for phishing events.
- Expand procedures for gathering evidence.
- Set up frequent tabletop exercises for phishing situations.

Relative Cost: Medium
Control Type: Forensic

Audit Controls

9.8 Phishing Simulation Results

Track and examine phishing simulation results to find areas needing work.

- Monitor and examine results from phishing simulations.
- Sort user groups with high risk.
- Change instruction according to outcomes.
- Keep track of modifications over time.

Relative Cost: Low-Medium
Control Type: Audit

9.9 Email Security Assessment

Review email security policies often.

- Examine email security mechanisms often.
- Check how well anti-phishing techniques work.
- Review and update email security rules.
- Analyze email security from the outside.

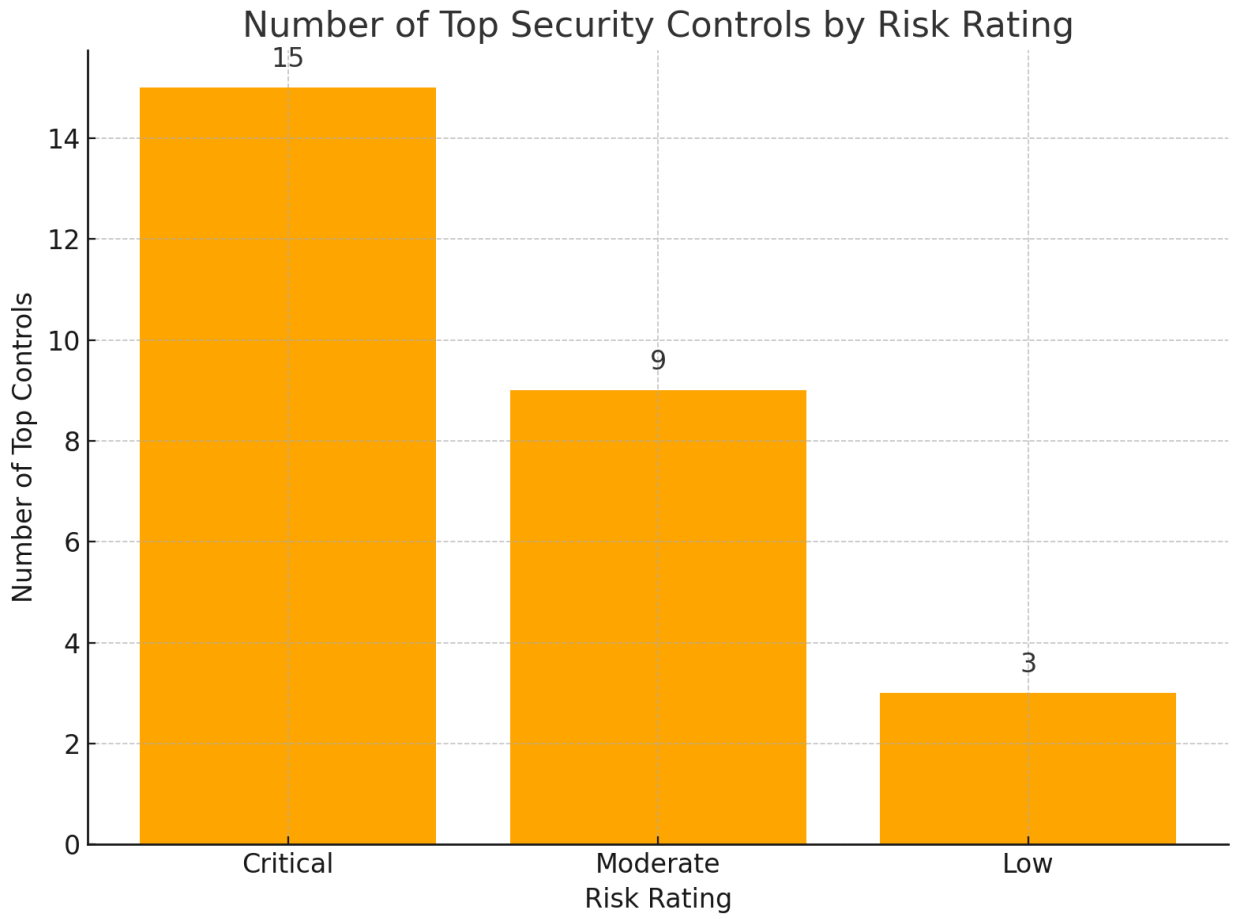
Relative Cost: Medium
Control Type: Audit

Ranked Security Controls

The following security controls have been ranked in decreasing order of efficacy based on the probability vs. impact matrix from the Part 2 risk assessment. Higher priority is given to controls addressing critical risks; the ranking corresponds with the risk ratings (Critical, Moderate, Low) found in the assessment.

Risk Category	Risk Rating	Control Effectiveness	Top Controls
Supply Chain Vulnerabilities	Critical	High	Vendor Assessment, Continuous Monitoring, Component Validation
GPU Driver Exploits	Critical	High	Regular Driver Updates, Driver Whitelisting, Driver Activity Monitoring
Firmware Vulnerabilities	Critical	High	Regular Firmware Updates, Firmware Validation, Secure Boot
Intellectual Property Theft	Critical	High	Confidential Computing, Access Control, Data Encryption
Ransomware Attacks	Critical	High	AI-Enhanced Security, Backup and Recovery, Network Segmentation
Server Vulnerabilities	Moderate	Medium	Patch Management, Secure Configuration, Vulnerability Scanning
DDoS Attacks	Moderate	Medium	Deep Learning-based DDoS Protection, Traffic Management, Rate Limiting
Insider Threats	Moderate	Medium	User Behavior Analytics, Access

			Control, Data Loss Prevention
Phishing Attacks	Low	Lower	AI-Enhanced Email Security, Multi-Factor Authentication, Security Awareness Training



As we can see from the graph, we need more critical controls; therefore, the urgent fix is to safeguard the infrastructure from various forms of attack.

Using the security controls described in this paper calls for careful preparation, budget allocation, and prioritizing. Implementation concerns—including cost analysis, implementation schedule, and resource needs—are discussed in this part under guidance.

Cost Analysis

Security control implementation includes direct financial expenses, personnel time, and possible operational effects among several expenses. Based on the recommended controls in this report, the relative expenses for every risk category are compiled in the following table:

Risk Category	Average Control-Cost	Implementation Complexity	Operational Impact
Supply Chain Vulnerabilities	Medium-High	High	Medium
GPU Driver Exploits	Medium	Medium	Low-Medium
Firmware Vulnerabilities	Medium	Medium	Medium
Intellectual Property Theft	High	High	Medium
Ransomware Attacks	High	High	Medium-High
Server Vulnerabilities	Medium-High	Medium	Medium
DDoS Attacks	Medium-High	Medium-High	Low-Medium
Insider Threats	Medium-High	High	Medium
Phishing Attacks	Medium	Low-Medium	Low

Cost Breakdown by Control Type

Different types of controls typically have different cost profiles

1. **Preventative Controls**: Though they can lower long-term incident response costs, preventative controls sometimes have higher upfront costs. Usually requiring large initial technological, configuration, and integration investments, these controls call for major technological knowledge.

2. **Detective Controls**: Usually have reasonable running expenses and initial outlay. These controls often involve the use of monitoring systems, log analysis tools, and staff to review alarms.

3. **Forensic Controls**: Usually have reasonable initial expenses, but maintaining and running can prove costly. These controls call for specific tools and educated staff members.

4. **Audit Controls**: Usually have more personnel costs but fewer technology expenses. These controls call for documentation, evaluations, and consistent reviews.

Cost Optimization Strategies

Through the following strategies, we can optimize the costs.

1. **Phased Implementation**: Prioritize critical controls and implement them first as much as the budget allows you, followed by moderate and low-risk controls.

2. **Leverage Existing Investments**: Instead of implementing new controls and strategies, try to extend the features of existing security tools, which can align with some of the needs.

3. **Consolidate Tools**: Try to consolidate security tools to reduce licensing, maintenance, and operational expenses.

4. **Automation**: Automate routine security tasks to reduce personnel costs and improve efficiency.

5. **Cloud-Based Solutions**: As per today's trend, try to manage your sources through cloud-based security services or move them according to your needs, some of the popular services being AWS and Azure.

Implementation Timeline

Security control implementation should be phased, giving important risks top priority and making sure the company can properly absorb the changes. The high-level road map for implementation is presented below.

Note: The timeline and phases for the month are imaginary and can vary based on actual company internal policies and budget.

Phase 1: Critical Risk Controls (0-6 months)

First, focus on implementing high-effectiveness controls for critical risks:

Month 1-2

- Apply due diligence and vendor assessment to supply chains.
- Create automated driver update control.
- Apply procedures for firmware validation.

- For sensitive systems, apply multi-factor authentication.

Month 3-4

- Use component validation in supply chains.
- Implement driver whitelisting.
- Provide a safe boot for firmware.
- Use intellectual property data encryption.
- Provide backup and recovery strategies for ransomware defense.

Month 5-6

- Put ongoing supply chain monitoring into action.
- Implement driver activity monitoring.
- Apply monitoring to firmware update activities.
- Provide network segmentation for ransomware defense.
- Include behavioral monitoring in use to find ransomware.

Phase 2: Moderate Risk Controls (7-12 months)

Next up, we need to address the moderate risks, so starting with month 7, we can do the following:

Month 7-8

- Put server patch management into use.
- Install a safe configuration on servers.
- Apply DDoS protection based on deep learning.
- Use user behavior analytics to identify insiders' threats.

Month 9-10

- Using vulnerability scanning on servers
- Apply traffic control for DDoS defense.
- Use access control to help insider threats.
- Implement insider threat protection by means of data loss prevention.

Month 11-12

- Put log monitoring for servers into use.
- Apply traffic analysis for DDoS protection.
- Install security awareness programs to help prevent insider threats.
- Test servers penetration-wise.

Phase 3: Low Risk Controls and Enhancements (13-18 months)

We are focusing on low risks, but we can enhance them using existing controls before the timeline is reached.

Month 13-14

- Use AI-powered email security to stop phishing.
- Set up email monitoring to find phishing.
- Improve current controls depending on the evaluation of their efficiency.

Month 15-16

- Put email authentication into use to stop phishing.
- Provide security awareness courses meant to prevent phishing.
- Improve and maximize already in-use controls.

Month 17-18

- Do thorough security evaluations.
- Solve any weaknesses or gaps.
- Create an enduring security roadmap.

Resource Requirements

Using the security measures described in this paper calls for different resources—people, technology, money, etc. The following summarizes the needs for resources.

Personnel Resources

Security Team

- Security architects to design and implement controls.
- Security analysts to monitor and respond to alerts.
- Security engineers to configure and maintain systems.
- Forensic specialists for incident response and investigation.

IT Team

- System administrators to implement and maintain controls.
- Network engineers to implement network-based controls.
- Database administrators secure database systems.
- Application developers to implement secure coding practices.

Business Team

- Project managers to coordinate implementation
- Business analysts to assess impact on business processes
- Change management specialists to manage organizational change
- Training specialists to develop and deliver security awareness training

Technology Resources

- Security Tools
- Vendor risk management platform
- Vulnerability scanning tools
- Security information and event management (SIEM) system
- Data loss prevention (DLP) solution
- User behavior analytics (UBA) platform
- Encryption solutions
- Backup and recovery systems
- Email security gateway
- Multi-factor authentication solution
- Penetration testing tools

Infrastructure

- Servers for security tools
- Network infrastructure for monitoring and protection
- Storage for logs and forensic data
- Cloud resources for cloud-based security services

Budget Considerations

The size of the company, present security posture, and particular needs will all affect the budget needed to apply the security controls. Still, the following offers a broad rule for financial distribution.

Technology Investment: 40-50% of the security budget

- Security tools and platforms
- Infrastructure upgrades
- Cloud services

Personnel: 30-40% of the security budget

- New hires or contractors
- Training and certification
- Professional services

Operations: 10-20% of the security budget

- Ongoing maintenance and support
- Subscriptions and licenses
- Incident response and recovery

Contingency: 5-10% of the security budget

- Unexpected costs
- Emergency response
- Regulatory compliance

NVIDIA can efficiently apply the security controls described in this report by well-planning and allocating resources, optimizing expenses, and maximizing security benefits.

Conclusion

Summary of Findings

Based on the vulnerabilities and risks found in the Part 2 risk assessment for NVIDIA, this all-encompassing security controls assessment has found and evaluated a broad spectrum of security controls to handle them. With relative cost estimates, the assessment classified nine main risk areas—from critical to low risk—and offered several control options for each risk, based on type (Preventative, Detective, Forensic, and Audit).

Supply chain vulnerabilities, GPU driver exploits, firmware flaws, intellectual property theft, and ransomware attacks on NVIDIA's AI infrastructure rank highest among the most critical risks found. These important hazards need quick attention and strong security measures since their possible negative effects on NVIDIA's operations and reputation could be rather severe.

The evaluation indicates that a layered defense approach, which includes several types of controls for each risk, yields the best security posture. While detective controls enable the identification of security events that evade preventative measures, preventative controls serve as the initial line of defense. The security architecture is completed by forensic and audit controls, which enable effective incident response and continuous improvement.

Key Recommendations

Based on the assessment findings, the following key recommendations are provided.

1. **Prioritize Critical Risks**: Concentrate the first implementation efforts on the controls handling important risks, especially those with high ratings of effectiveness. These include checking vendors and doing background checks for supply chain weaknesses, regularly updating drivers and allowing only safe GPU drivers, validating firmware and ensuring safe booting to protect against firmware issues, using secure computing and access controls to protect intellectual property, and implementing AI-based security and backup systems to guard against ransomware.

2. **Implement a Balanced Control Profile**: Apply a balanced portfolio of controls spanning all four control types—Preventative, Detective, Forensic, and Audit—for every risk to guarantee thorough protection. This method guarantees that, should one control fail, others are ready to reduce the risk and offers defense-in-depth.

3. **Adopt a Phased Implementation Approach**: Start with high-effectiveness controls and critical risks, then move through phases including modest and low risks using security controls. This strategy guarantees that the most important hazards are taken care of first and lets the resources be allocated effectively.

4. **Leverage NVIDIA's AI Capabilities**: Use NVIDIA's strengths in GPU technology and artificial intelligence to improve security measures. Leveraging NVIDIA's core competencies, AI-enhanced security solutions, including deep learning-based DDoS protection and phishing detection, can offer notable security advantages.

5. **Establish Continuous Monitoring and Improvement**: Use ongoing security control monitoring to evaluate their performance and spot areas needing work. Review and update security controls often depending on new threats, shifting risk terrain, and lessons discovered from security events.

6. **Invest in Security Awareness and Training**: Create thorough security awareness campaigns for every staff member, including specialized instruction for those managing sensitive data or systems. Security is much influenced by human elements; thus, well-trained staff members can be excellent security control agents.

7. **Develop Comprehensive Incident Response Capabilities**: With particular policies, tools, and trained staff for every type of risk, build strong incident response capability for all found risks. When security events transpire, good incident response can greatly lessen their impact.

Future Considerations

As NVIDIA continues to evolve its security posture, the following future considerations
It should be taken into account.

- **Emerging Threats**: Track constantly for new risks and weaknesses that might affect NVIDIA's products, operations, or processes. Change security levels as necessary to handle fresh risks.

- **Technological Advancements**: Keep up with developments in security technology, especially in fields pertinent to NVIDIA's operations, including supply chain security, confidential computing, and AI-enhanced security. Review and apply new security technologies as suitable.

- **Regulatory Changes**: Track changes in laws that might affect NVIDIA's security responsibilities. Make sure security policies reflect current compliance with pertinent rules.

- **Business Evolution**: As NVIDIA's business changes, review the risk environment and modify security policies. New goods, services, or business models could bring fresh risks that call for different kinds of security measures.

- **Security Metrics and Measurements**: Create thorough security metrics to evaluate the general security posture and security control effectiveness. These benchmarks will help you show the worth of security expenditures and propel ongoing development.

NVIDIA can greatly improve its security posture and safeguard its valuable assets, intellectual property, and infrastructure from cyber threats by applying the advised security controls and thinking through these future directions.

References

1. NVIDIA Developer. "Supercharge Ransomware Detection with AI-Enhanced Cybersecurity Solutions." NVIDIA Developer Blog, 2024. https://developer.nvidia.com/blog/supercharge-ransomware-detection-with-ai-enhanced-cybersecurity-solutions/

2. NVIDIA. "Morpheus Cybersecurity Solutions." NVIDIA Developer, 2024. https://developer.nvidia.com/morpheus-cybersecurity

3. NVIDIA Corporation. "NVIDIA Security Bulletin: Multiple Vulnerabilities in GPU Display Driver." NVIDIA, February 2025. https://www.nvidia.com/en-us/security/

4. BlueVoyant. "Supply Chain Security: Why It's Important & 7 Best Practices." BlueVoyant Knowledge Center, 2024. https://www.bluevoyant.com/knowledge-center/supply-chain-security-why-its-important-7-best-practices

5. ISO/IEC. "ISO/IEC 27001:2022 Information Security Management Systems — Requirements." International Organization for Standardization, 2022.

6. NIST. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1." National Institute of Standards and Technology, April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

7. NVIDIA. "NVIDIA AI Cybersecurity Solutions for your Business." NVIDIA, 2024. https://www.nvidia.com/en-us/solutions/ai/cybersecurity/

8. NVIDIA Corporation. "NVIDIA Security Bulletin: Multiple Vulnerabilities in GPU Display Driver." NVIDIA, February 2025. https://www.nvidia.com/en-us/security/

9. Massed Compute. "What are the best practices for securing NVIDIA data center GPU drivers against malware and viruses?" Massed Compute FAQ, 2024. https://massedcompute.com/faq-answers/?question=What+are+the+best+practices+for+securing+NVIDIA+data+center+GPU+drivers

10. Massed Compute. "What are the best practices for securing NVIDIA GPU firmware updates?" Massed Compute FAQ, 2024. https://massedcompute.com/faq-answers/?question=What+are+the+best+practices+for+securing+NVIDIA+GPU+firmware+updates

11. NVIDIA Developer. "Protecting Sensitive Data and AI Models with Confidential Computing." NVIDIA Developer Blog, 2024. https://developer.nvidia.com/blog/protecting-sensitive-data-and-ai-models-with-confidential-computing/

12. Netwrix. "Insider Threat Prevention Best Practices." Netwrix, 2024. https://www.netwrix.com/insider-threat-prevention-best-practices.html

13. NVIDIA Developer. "NVIDIA Morpheus Helps Defend Against Spear Phishing with Generative AI." NVIDIA Developer Blog, March 2023. https://developer.nvidia.com/blog/nvidia-morpheus-helps-defend-against-spear-phishing-with-generative-ai/

14. NVIDIA. "Spear Phishing Detection AI Workflow." NVIDIA, 2024. https://www.nvidia.com/en-us/ai-data-science/ai-workflows/spear-phishing/

15. Phish Protection: "Top 10 Phishing Prevention Best Practices For Safe Corporate Environment." Phish Protection Resources, 2024. https://www.phishprotection.com/resources/top-10-phishing-prevention-practices

16. CybeReady. "10 Phishing Prevention Best Practices the Pros Swear By." CybeReady, October 2023. https://cybeready.com/phishing-awareness-training/phishing-prevention-best-practices