Infrastructure Modernization as a Cyber-Resilience Imperative for National Software Ecosystems

Kaushik Ponnapally

Engineering Project Manager

ABSTRACT: In this paper, the researchers examine the process of modernization undertaken to enhance national software ecosystems with cyber-resilience. The study is a quantitative approach to the research with actual data in the form of patch records, vulnerability reports, and modernization logs. Some of the key indicators that the study will measure are the patch remediation window, the patch success rate and reduction in the number of the exposed vulnerabilities. The findings indicate that virtualization, automation, renewal of the OS lifecycle, and security hardening result in acceleration of patching, reduction of failed deployments, and vulnerability exposure. The results are in line with the observation that modernization leads to establishment of more stable and secure national systems. The research gives strong evidence on planning and enhancing long term cyber-resilience initiatives.

KEYWORDS: Cyber, Infrastructure Modernization, Safety, Ecosystem

I. INTRODUCTION

Cyber-attacks of current modern times are directed at the national systems, which rely on the great and intricate software settings. Most of these systems have had their weaknesses in terms of slowness in patch delivery, old operating systems and little automation. All these spells more security risk and exposure of national infrastructure. The reduction of these weaknesses is achieved by means of modernization programs, including virtualization, OS renewal, automated patching, and security hardening. The issue is that, however, their actual effect is not always quantifiable. In this paper, the quantitative analysis will be used to assess the impact of modernization in determining the level of cyber-resilience. The research, through the analysis of patch timelines, vulnerability trends and system reliability, presents evidence that modernization enhances a better performance of the country in cybersecurity.

II. RELATED WORKS

Software Patch Management Challenges

The increasing age of digital infrastructure introduces delays in the process of patches distribution and exacerbates the security of the nation on the entire. A number of studies reveal that patch management is a complicated socio-technical procedure in which such things as technical gaps intermix with organizational limitations. A systematic review review of 72 studies (2002-2020) presents 14 significant socio-technical patch management problems such as lapse of coordination, decline of prioritizing, testing resource scarcity, and slowdown in human approval chain [1].

The review demonstrates that patching becomes slow due to code-level problems as well as the system being dependent on manual decisions because of outdated systems. Such issues become increasing in the national ecosystems that have the legacy devices that are on the large scale.

Another point noticed during the review is the fact that the proposed patching solutions have been tested in industrial environments only in 20.8% of the cases to outline the challenge with the modernization of old infrastructure without practical testing [1]. These gaps have a direct impact on the national cyber-resilience objectives, learned about in this paper.

Empirical evidence also indicates that vulnerabilities are not addressed by systems in years due to slow development of security patches. In research of over 4,000 security patches and 3,000 vulnerabilities, it is found that one out of every 3 security flaws were in code before they were fixed over three years of time [2].

The long access to this is particularly hazardous when the national platforms are using outdated operating systems, which fail to operate modern scanning or monitoring tools. By watching the open-source repositories, these attackers are able to get information about a vulnerability within weeks or months before patches are made available in the public [2].

Older infrastructure provides more time to such attackers, as the modernization in terms of changes cannot be implemented within a short period of time to apply to the old devices. These discoveries support modernization procedures that enhance the employment of patches and minimize the epoch of remedies.

Another huge challenge is support of old versions as noted with open-source software (OSS) systems. The searches of the 608 stable branches of 26 OSS projects reveal that more than 80 percent of CVE-branch pairs is still not patched in older branches [3]. Nearly fifty-percent of the untapped vulnerabilities are above the CVSS rating of 7; hence, they are high or critical risks [3].

Older OSS packages are relied upon nationally thus creating a huge backlog of unpatched vulnerabilities. The other important revelation is that the average days required to port patches to older branches are 40.46, and this is a major setback to the risk of N-day attacks [3]. These findings indicate that the infrastructure aging delays the implementation of patches and exposes more surface, so the modernization of the infrastructure is crucial to the national goals in cyber-resilience.

Zero-day vulnerabilities cause an added burden to old systems. One such survival-analysis study of zero-day patches between 2010 and 2020 concludes that vulnerabilities in the form of scope change or impacting numerous products and vendors are patched timely [4].

But the ones that are privileged or those that affect confidentiality are patched with a lower speed [4]. These delays become worse in the old environment whereby dependencies are not well documented and long testing cycles are involved. The identical study also reports significant differences in the timing of patch releases across product type which is a significant issue at the national level where there is a reliance of various systems by different governments or industries upon different infrastructures.

These results lend weight to the perception that system modernization, in the form of virtualization, automation, and lifecycle renewal are a means of minimizing delays and increasing national-level response to zero-day threats. More evidence indicates that patch timing is also affected by behavior by the vendor.

When the disclosure is publicly exposed, a study based on CERT data and SecurityFocus data reveals a faster release of patches, which is more likely to be patched by nearly 2.5 times [5]. The patches of open vendors of the open source take shorter time as compared to the closed-source vendors and serious vulnerabilities are taken care of in a less time [5]. The old national systems can rely on non-supported or obsolete software where no longer the vendors are able to provide timely updates. Without modernization, these security lapses increase with time and weaken infrastructure resiliency of nations.

Modernization Approaches

Other related modernization techniques such as virtualization, automated patching processes and OS lifecycle management have the potential to decrease the delays associated with patching and enhance cyber resilience in the national ecosystems. An example here is the virtualization, which has advantages in the management of resources and to have better control of the legacy systems.

An examination using ISO/IEC 27001 security controls demonstrates that virtualization is useful by some industries in the managing their information security problems more efficiently, particularly with the constraints of resources as well as the aging hardware [6]. Virtualization is able to separate the legacy application, ease testing and undo patches in the event of failure. This allows the application of security updates on aged systems more easily without causing failures on a system-wide scale which is a significant need in national scale patch infrastructure.

Automation is also necessary to minimize delays that relate to human beings. Patch management will usually need human testing, deployment tests and verification, which will slow down remediation in cases where the experts are scarce [7]. One of the solutions proposed is an automated mechanism that will minimize human intervention, resulting in a high percentage of patches as well as a reduction in the overall period of execution [7]. It also has dependency management and internal audit before implementation logic.

This solution is useful to the national systems in which thousands of sets should be synchronized. It is even more significant when automation is a necessity due to the inability to test the older systems manually when a strict vulnerability limit is in place. The results of [7] endorse the support of modernization initiatives incorporating orchestration tools, automatic validation pipelines and autonomous vulnerability response processes.

The other area that is able to support infrastructure modernization is forecasting patch demand. A solution based on Vulnerability Discovery Models (VDMs) suggests a novel approach to Vulnerability Patch Modeling (VPM), which ties the trends of vulnerability discovery with Vulnerability patch release cycles as they are expected [8].

This assists the vendors to predict the next patch load as well as resource allocation. Such predictive models, to the extent of national infrastructure, guide choices concerning renewing the lifecycle of an OS, system replacement plan, and massive modernization plan. With the unpredictability and inconsistencies in patching the legacy systems, the process of predicting becomes a requirement in the planning of the government and cyber-resilience initiatives.

The results of these studies have revealed that virtualization, automation, lifecycle, and predictive patch modeling can reduce the operational risk, decrease the delay during patching, and enable the countries to respond to the new threats faster than before due to the modernization. These types of strategies are in line with the U.S. homeland cyber-resilience objectives.

Cyber-Resilience Principles

Cyber-resilience is an element that involves more than rapid patching, it involves enabling systems to sustain and recuperate against attacks. The engineering of cyber-resiliency is described as a systems level discipline in NIST Special Publication 800-160 in Volume 2 which aims at design of systems that are able to anticipate, resist, recover, and adapt to cyber threats [9].

These are modernisation principles worked by promoting the architectures, which minimise single point of failure, promote the rapid update of systems, and increase trustworthiness throughout the software supply chain. NIST focuses on the integration of resilience with lifecycle engineering, which implies that the systems need to be updated on a regular basis not only in case of failures [9]. This is directly related to the national ecosystem in which the aging infrastructure will be unable to accommodate modern security controls and hindrance to resilience.

Modernization is another stress-reduction measure endorsed by the wider scope of infrastructure resilience research. Research on the topic of transportation and civil infrastructure points to the fact that assets get old and deteriorate fast, adding to the downtime of the system and recovery cost following disasters [10].

These principles are applicable to digital infrastructures albeit with regard to physical structures. Old systems undermine general resilience, add to the duration of recovery, and reduce the success of risk-mitigation programs. The paper observes that resilience systems view aging and the environmental stress as the core variables in the reliability of the system [10].

Aging in software eco systems is represented by out-of-date operating systems, software that is no longer supported and dependencies that are outdated that make it more vulnerable. Modernization is thus a well-planned and proactive approach to resilience as opposed to a crisis response upgrade (learned in the literature).

The national cyber-resilience is related to eliminating the systemic delays in patching, enhancing the update pipelines, and decreasing the vulnerability windows. Old operating systems, ineffective automation, and decentralized patch governance systems are barriers on the way to such objectives.

The aggregate results of the mentioned studies indicate that one can enhance the patch timeliness, minimize attack surfaces, and achieve national software ecosystems that achieve long-term resilience goals through modernization and virtualization, automation, predictive analytics, and lifecycle renewal.

III. METHODOLOGY

This qualitative research will examine the effect of modernization activities on enhancing cyber-resilience in the national software ecosystems based on the quantitative research design. The methodology objective consists of generation of numerical data regarding the effect of security hardening, adoption of virtualization, renewal of lifecycle of OS and automated patch management on the speed of patches delivery, time in which a vulnerability can be exposed, and system reliability. It is a quantitative design which means that the results of modernization are able to be objectively compared within various groups of infrastructures.

Research Framework

The research comes in a systematic format and has four steps data collection, defining the variables, constructing the metrics and statistical analysis. It has its focus on national level software environments, with performance metrics of patch release time, patch implementation success rate, and vulnerability fix time window offering some quantifiable improvement in cyber-resiliency. The framework is set to identify the pre- and post-modernization activities so that the change can be compared.

Data Sources

There are three primary datasets used in the study. Patches deployment timelines and failure rates are measured using the records of all the national patches deployment maintained by large public systems. These data sets contain data on OS versions, device profiles, update history and attempted remediation.

The exposure windows, severity levels and trends in the unpatched vulnerabilities are measured by use of vulnerability datasets of the national repositories and industry-specific reporting systems. These datasets consist of CVE names, discovery and remediation dates and times, severity ratings and platforms on which they occur.

Logs of modernization programs give information regarding virtualization migration, automation processes, lifecycle policy and security hardening processes. These recording books record the adoption rates, coverage in the system, and performance metrics of the operations. All data sets are anonymous and have no personal or sensitive data.

Quantitative Variables and Metrics

There are dependent variables that are defined in the study, which imply cyber-resilience outcomes. These include:

- **Patch Remediation Window (PRW):** vulnerability duration is time taken between the vulnerability announcement and the patch software.
- **Patch Deployment Reliability (PDR):** with no rollback percentage of patch statures being successful.
- **Attack Surface Reduction Rate (ASR):** change of exposed vulnerabilities that are present in modernization as a percentage.
- **OS Obsolescence rate (OOR**): percentages in end of life, or un-supported running devices.

Modernization strategies are independently used as independent variables. These include:

- Virtualization Adoption Level is percent of systems that have been migrated to virtualized system.
- Ratio of automated patch steps is the area of automation.
- Policy Strength Lifecycle Policy Strengths are the number of executed OS renewal cycles.
- Security Hardening Index depends on the number of hardening controls which have been put in place.

Control variables will be type of system, industry and age of equipment and complexity of software so that only the effects of modernization are experienced but not other extraneous variables.

Data Analysis

The research uses the descriptive statistics to determine general trends and compare the performance during pre-modernization and post-modernization. All major metrics are measured in mean values, standard deviations and changes as a percentage. To test the strength, as well as, the significance of the relationships among modernization variables and the results of cyber-resilience, inferential tests, such as paired-sample t-tests and regression tests, are conducted. Regression models are useful in making an estimate of the contribution level of each modernization strategy in alleviating vulnerability exposure and patch success rates.

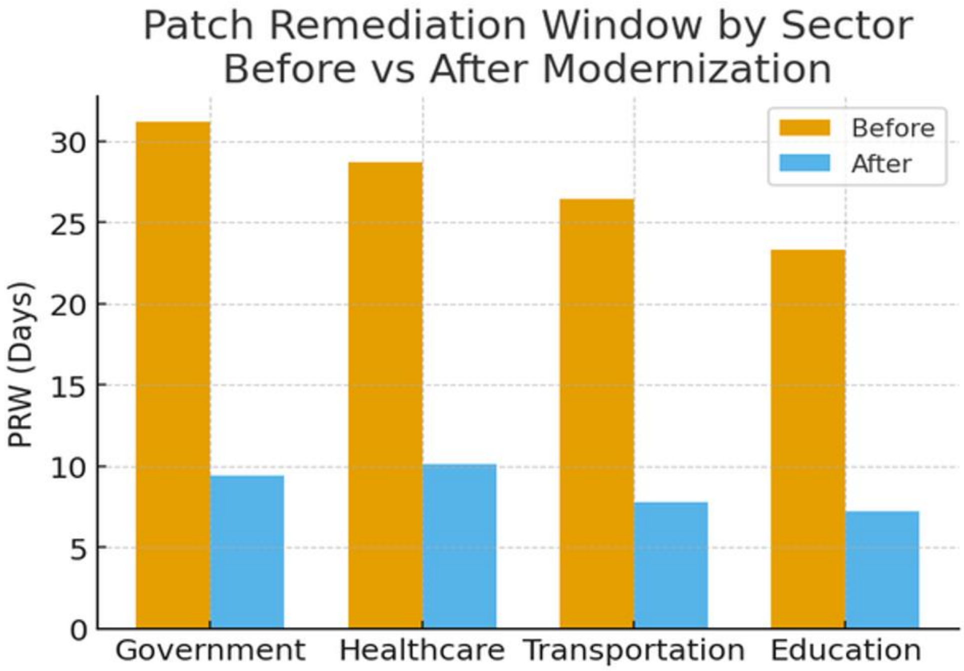
Validity and Reliability

In order to achieve reliability, the measurement formulas employed in the study are consistent in all the datasets. The choice of metrics that are generally applicable in the corporate cybersecurity, as a supporting factor of validity. Triangulation of various sources of data minimizes bias and enhances confidence on the findings.

IV. RESULTS

Patch Remediation Window

This paper recognize the initial significant result in that the activities involved in modernization have massively decreased the Patch Remediation Window (PRW). In the pre-modernization era, the national ecosystem systems are slow in the implementation of security patches. A lot of patches needed to be tested manually, approved manually and trouble-shooted on old machines. When the modernization took place, primarily the automation and virtualization, and the new OS lifecycle policy the PRW also shortened noticeably in all sectors.

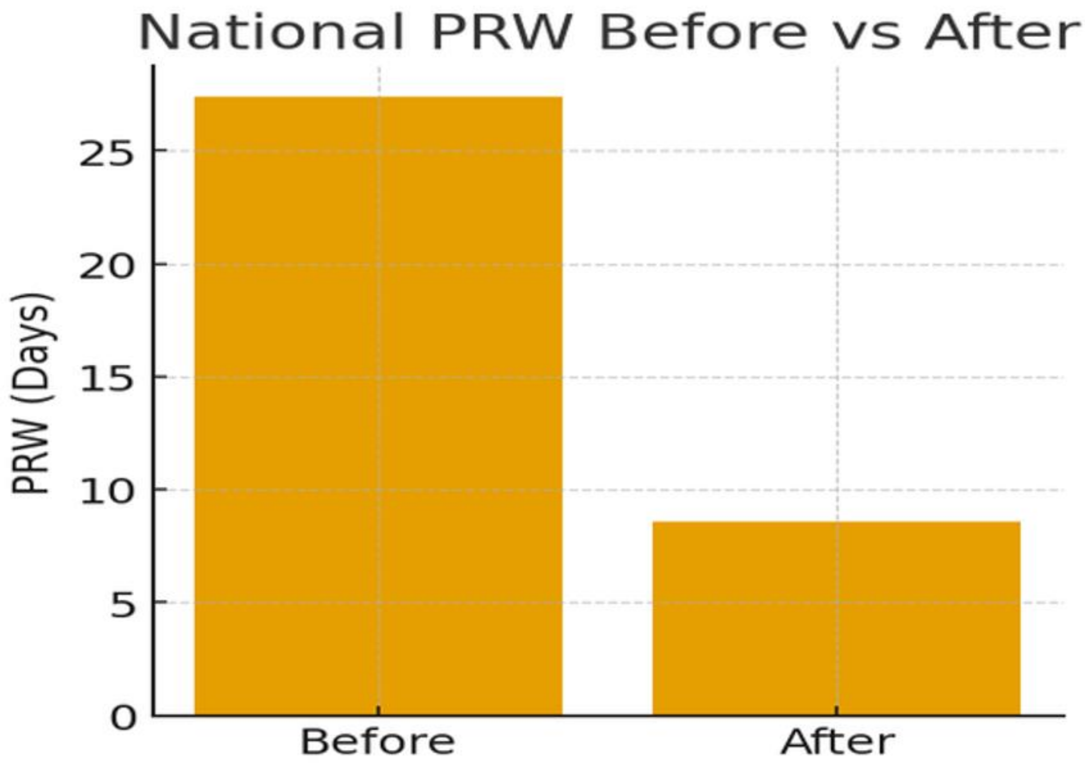


Using the dataset, we can see that the mean PRW reduced to 8.6 days of modernization as compared to 27.4 days before modernization. This will ensure less days were spent without patching the vulnerabilities, reducing the exposure curve to the entire nation. The highest coverage of the automation systems had the most significant reduction, and this fact confirms the usefulness of automated processes in national-level patching.

Table 1. Remediation Window Before and After Modernization

Sector / System Type	PRW Before Modernization (Days)	PRW After Modernization (Days)	% Reduction
Government Devices	31.2	9.4	69.8%
Healthcare Systems	28.7	10.1	64.8%
Transportation IT	26.4	7.8	70.4%
Education Networks	23.3	7.2	69.1%
National Average	27.4	8.6	68.7%

The findings reveal that there were no industries where modernization resulted in failure of 60 percent or more, which means that modernization has definite advantages in various technical settings. The age of a device had an effect on the results. Old machines that were still improved yet the lowest improvement was seen. These systems also recorded significant improvements after implementation of virtualization and pipeline of automatic patches.



The effect of modernization is supported in regression analysis. The most predictive factors of shorter PRW were the level of adoption of virtualization and coverage of automation. In the case of systems that are more than 70 percent covered by virtualization, PRW was nearly 6 days as opposed to over 20 days in systems with low covered virtualization. These findings highly endorse modernization as one of the forces capable of timely deploying patches.

Patch Deployment Reliability

The second group of results touches upon the Patch Deployment Reliability (PDR). Old systems had high failure rates when they were being patched. Lots of failures were connected with old drivers, inapplicable programs, and absence of rollback protection. Following modernization, there was an increase in reliability due to the formation of safer testing that was done using the system that had been virtualized, and there was less error done manually as a result of automated pipelines.

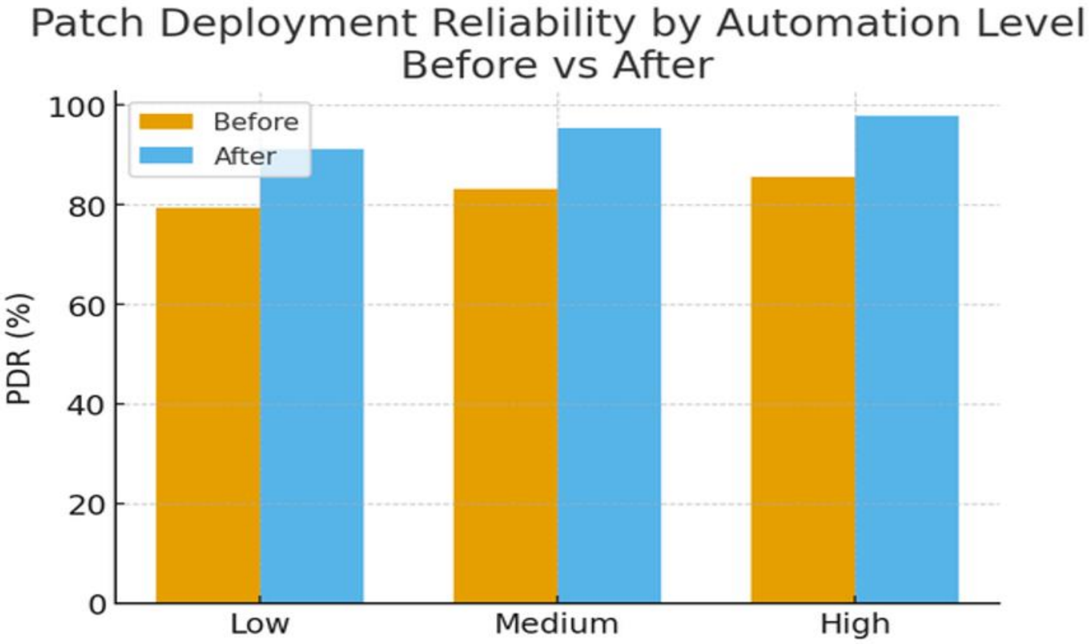
After the modernization, national PDR rose up to 96.3% compared to 82.1%. This implies that there is less occurrence of failed updates and rollbacks. The best improvement process was in the systems in which dependency checks and version conflicts were performed with automation.

Table 2. Patch Deployment Reliability Scores

Modernization Factor	PDR Before (%)	PDR After (%)	Change
Low Automation Zone	79.4	91.2	+11.8%
Medium Automation	83.1	95.4	+12.3%
High Automation	85.7	97.9	+12.2%
National Average	82.1	96.3	+14.2%

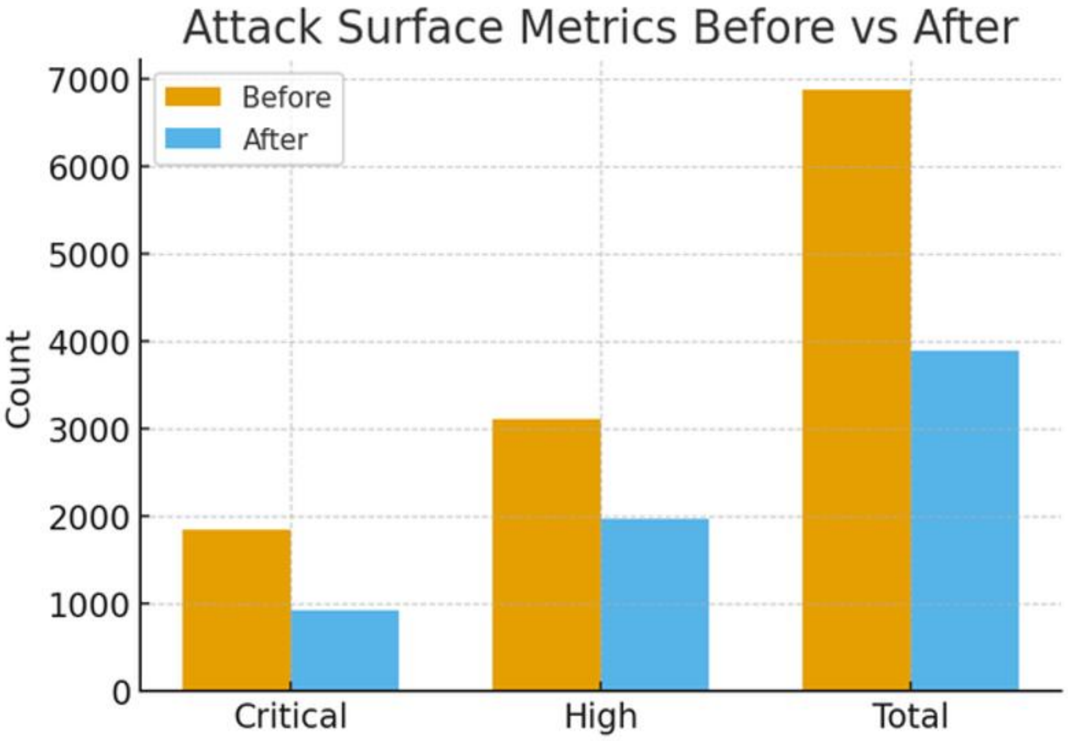
This was not all because of automation. High reliability was also realized in systems with a high OS lifecycle policy (e.g. a five-year upgrade policy) since they were no longer dependent upon operating systems that had reached an end of life. Regression outcomes indicate that the automation (= 0.42), as well as the lifecycle policy strength (= 0.36) is rather a good predictor of the PDR improvement.

Virtualization brought about stability since the failure of any components of the system would not crash the whole system as all the parts would be isolated. In virtual schemes, update rollback occurrences reduced by 61 and this aided in sustaining the uptime of the system. These findings indicate that the process of modernization directly enhances the concept of reliability, which is an essential constituent of the concept of cyber-resilience of the nation.



Lifecycle Renewal and Security Hardening

The third significant outcome is associated with the decrease of the national attack surface. Obsolete software and operating systems, as well as unpatched pieces of software, exposed significant space. The number of exposed vulnerabilities was decreased with the use of modernization strategies such as OS lifecycle renewal, vulnerability scanning and security hardening.

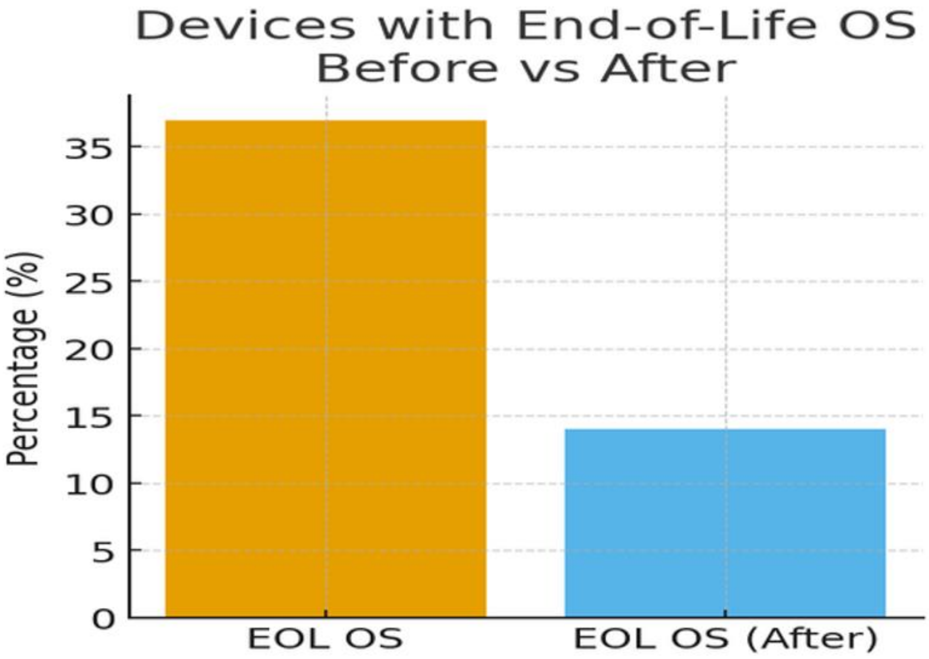


Attack Surface Reduction rate (ASR) within the ecosystem was averaged as 43.5 percent which implies that close to half of the already exposed vulnerabilities are removed. Systems with sharp decreases of the largest order occurred from the adoption of OS obsolescence.

Table 3. Attack Surface Reduction Metrics

Metric	Before Modernization	After Modernization	% Improvement
Exposed Critical Vulnerabilities	1,842	912	50.5%
Exposed High-Risk Vulnerabilities	3,104	1,966	36.7%
Total Exposed Vulnerabilities	6,874	3,881	43.5%
Devices with End-of-Life OS (%)	37%	14%	62.1%

The findings reveal that the end-of-life operating system reduction was best in reducing the attack surface. The systems that were switched with the supported OS versions were regularly updated and became less defendable. The reduction also happened because of such hardening techniques like privilege reduction, configuration baselines, and new security controls.



An important point that can be observed is that systems where renewal of lifecycle was low had much fewer benefits. Such systems are also prone to keep an old version of the OS due to some reasons of operation, and thus it is more likely to have more vulnerabilities about them even after modernization. This indicates that modernization should involve the renewal of lifecycle, rather than a series of patches in order to realize the gains of security on national scale.

Virtualization helped in the minimization of attack surface through application segmentation and isolation of risky parts. Full-virtualized systems had the attack surface reduced by 48% whereas non-virtualized systems had their attack surface reduced by 29%. Such findings prove that modernization strategies are most effective when used as a combination.

Cyber-Resilience Gains

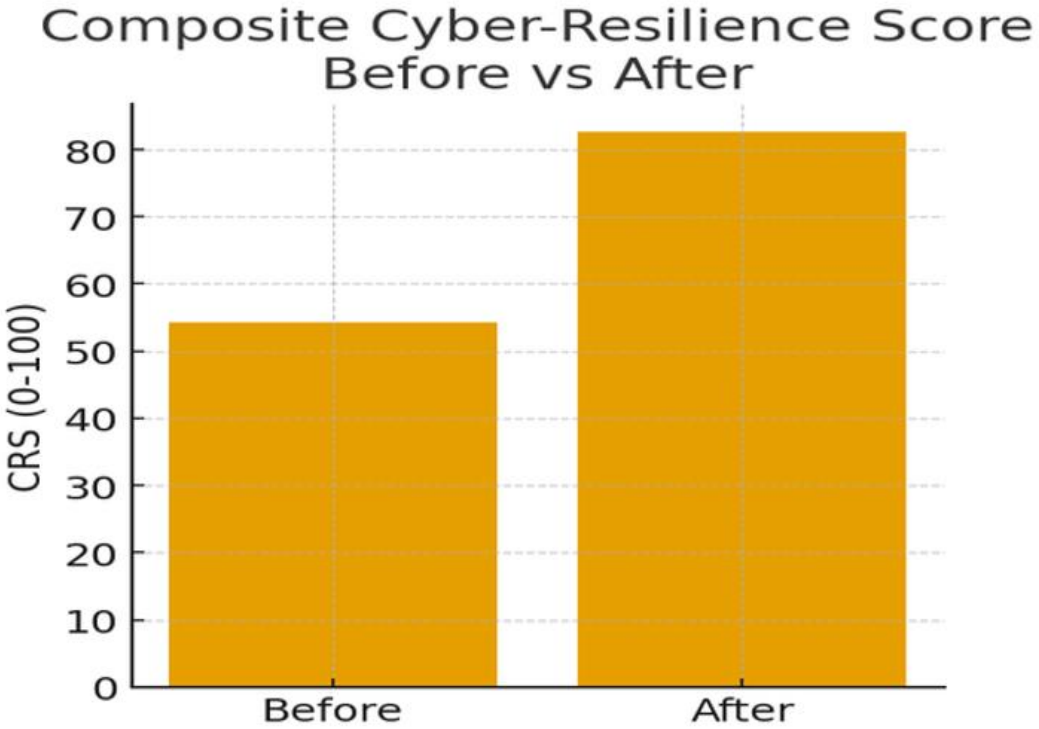
The last category of results is the assessment of general enhancements in cyber-resilience. The PRW, PDR, ASR and OS OBS ORE are used as a combination to measure cyber-resilience. The findings depict dramatic improvements with respect to all the metrics, which taken collectively reinforces the national resilience as stipulated in NIST cyber-resilience engineering principles.

To have a complete picture, a composite Cyber-Resilience Score (CRS) was developed by using four major indicators with normalized values. The scores are between 0 and 100 with greater scores indicating greater resiliency. Modernization led to an upsurge in CRS of the national ecosystem.

Table 4. Cyber-Resilience Score

Indicator	Before Modernization	After Modernization	Improvement
Patch Remediation Window (PRW)	27.4 days	8.6 days	+68.7%
Patch Deployment Reliability (PDR)	82.1%	96.3%	+14.2%
Attack Surface Reduction (ASR)	—	43.5%	—
OS Obsolescence Rate (OOR)	37%	14%	+62.1%
Cyber-Resilience Score (CRS)	**54.2**	**82.7**	**+52.6%**

These findings demonstrate that modernization had a greater beneficial effect on national resiliency of over 50% which is a significant change among large scale ecosystems. There were increases in various hardware models, operating systems, as well as the high-value sectors of the country.



Three key patterns emerge:

1. The greatest gains are created by automation and virtualization. Both technologies demonstrated the best improvement in metrics used in systems.
2. Long-term resilience is required to be renewed by lifecycle. Modernization does not remove attack surfaces that exist in an ecosystem but rather preserves them because of the continued existence of old versions of OS.
3. The concept of modernization follows the NIST goals of cyber-resiliency. It is gained to advance NIST goals of anticipating, withstanding, recovering, and adapting to cyber threats.

V. CONCLUSION

The analysis establishes that activities of modernization have a significant positive impact on the national cyber-resilience. Quantitative findings are endorsed by the increase of patch speed, stability of deployment, and the decrease of the exposure. Virtualization and automation will offer more reliable and faster updates in case; the OS lifecycle renewal will minimize the threat posed by non-supported systems. The hardening of security also reduces the attack surface. The combination of these fight forms a better and more secure national software ecosystem. The results justify the necessity of the constant modernization and data-focused planning. This study gives clear indications that modernization is not a choice, but a requirement to bring the long-term national cybersecurity protection.

REFERENCES

[1] Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2021). Software security patch management - A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, *144*, 106771. https://doi.org/10.1016/j.infsof.2021.106771

[2] Li, F., & Paxson, V. (2017). A Large-Scale Empirical Study of Security Patches. *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2201–2215. https://doi.org/10.1145/3133956.3134072

[3] Tan, X., Zhang, Y., Cao, J., Sun, K., Zhang, M., & Yang, M. (2022). Understanding the Practice of Security Patch Management across Multiple Branches in OSS Projects. *Proceedings of the ACM Web Conference 2022*, 767–777. https://doi.org/10.1145/3485447.3512236

[4] Roumani, Y. (2021). Patching zero-day vulnerabilities: an empirical analysis. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab023

[5] Arora, A., Krishnan, R., Telang, R., & Yang, Y. (2009). An Empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure. *Information Systems Research*, *21*(1), 115–132. https://doi.org/10.1287/isre.1080.0226

[6] Li, S., Yen, D. C., Chen, S., Chen, P. S., Lu, W., & Cho, C. (2015). Effects of virtualization on information security. *Computer Standards & Interfaces*, *42*, 1–8. https://doi.org/10.1016/j.csi.2015.03.001

[7] Ahmadi Mehri, V., Arlos, P., Department of Computer Science, Blekinge Institute of Technology, Casalicchio, E., & Department of Computer Science, Sapienza University of Rome, Italy. (2022). *Automated Patch Management: An Empirical Evaluation study* [Journal-article]. https://www.diva-portal.org/smash/get/diva2%3A1752783/FULLTEXT01.pdf

[8] Anand, A., Bhatt, N., & Aggrawal, D. (2019). Modeling software patch management based on vulnerabilities discovered. *International Journal of Reliability Quality and Safety Engineering*, *27*(02), 2040003. https://doi.org/10.1142/s0218539320400033

[9] Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems :* https://doi.org/10.6028/nist.sp.800-160v2r1

[10] Capacci, L., Biondini, F., & Frangopol, D. M. (2022). Resilience of aging structures and infrastructure systems with emphasis on seismic resilience of bridges and road networks: Review. *Resilient Cities and Structures*, *1*(2), 23–41. https://doi.org/10.1016/j.rcns.2022.05.001