

From Safety to Cybersecurity

Engineering Protection for National and Economic Security

Dr. Ron Ross

CEO, RONROSSECURE, LLC
ISTS FELLOW, DARTMOUTH COLLEGE

Abstract

Aviation and automotive safety demonstrate how regulation, market incentives, engineering, and visible evidence can reinforce one another. Modern cybersecurity shares those needs but introduces adaptive adversaries, rapidly changing software, concentrated digital dependencies, and consequences that can extend across organizations and sectors. Drawing on the author's articles "Trustworthy Secure Design" and "Adequate Security," this article extends the historical comparison to the protection of essential services and national and economic security. It argues that private risk decisions must account for public consequences, that protection must begin with system architecture, and that confidence must be supported by evidence proportionate to the losses at stake. The policy recommendations are an analytical synthesis rather than a claim that the cited engineering guidance prescribes a particular regulatory model.

1. Introduction

The development of aviation and automobile safety offers a useful starting point for examining cybersecurity. Both industries made progress through an interaction of engineering innovation, government requirements, liability, and market incentives. What can their experience teach us about protecting the computer systems on which modern society depends?

This article argues that the same reinforcing forces are needed in *cybersecurity*, but must address adaptive adversaries, shared digital dependencies, and losses that can extend far beyond the organization operating a system. Trustworthy secure design and evidence-based judgments of adequate security provide an engineering foundation for that response. When essential services and national missions are at stake, private risk acceptance must be evaluated against public consequences.

Neither government intervention nor private sector incentives operated in isolation. Financial exposure, consumer expectations, engineering innovation, and federal action influenced one another. Their relative importance differed between industries and changed over time.

The central lesson is that *incentives* become more effective when buyers can evaluate protection and when minimum requirements prevent essential safeguards from being treated solely as optional costs.

"Visible evidence of safety strengthens the market incentive to improve it."

2. Airline and Commercial Aviation Safety

In commercial aviation, safety is fundamental to passenger confidence and commercial viability. Strong financial incentives nevertheless coexist with the need for uniform rules, shared infrastructure, and continuing oversight.

Market and Private Sector Incentives

- **Customer trust as a core asset.** Passengers depend on the carrier, aircraft manufacturer, crews, maintenance organizations, and supporting infrastructure. A catastrophic accident can damage confidence and create substantial financial and liability exposure.
- **Capital and operational costs.** Aircraft are major investments. Aircraft losses, disrupted operations, and reputational damage create powerful reasons to prevent accidents and improve reliability.
- **Early industry support for regulation.** According to the FAA's historical account, aviation leaders supported federal action to improve safety and enable commercial growth. Their advocacy helped bring about the Air Commerce Act of 1926, which established federal responsibilities for pilot licensing, aircraft certification, airways, and air traffic rules [1].

Government Driving Force

- **Uniform infrastructure and oversight.** Shared airspace requires coordinated rules and services. Federal oversight established a common framework for certification, operations, and air navigation. The Federal Aviation Act of 1958 created the agency that became today's FAA [1].
- **Learning from accidents.** Accidents and operational experience exposed weaknesses that required coordinated corrective action. On June 30, 1956, TWA Flight 2 and United Airlines Flight 718 collided over the Grand Canyon, killing all 128 people aboard. The FAA identifies the collision as a major catalyst for air traffic control reform and creation of the Federal Aviation Agency under the Federal Aviation Act of 1958 [9]. The case demonstrates how a failure in a shared aviation operating system can require coordinated engineering and public action.

Aviation therefore illustrates how strong market incentives can support regulation rather than eliminate the need for it. Common standards strengthen confidence across a system whose safety depends on many interacting organizations.

3. Automobile Safety

In the automobile industry, safety competed with styling, performance, comfort, and price. Voluntary innovation demonstrated that safer designs were possible, but innovation alone did not ensure that protections became standard across vehicles.

The Initial Market Challenge

- **Safety as a difficult selling proposition.** Buyers could readily compare price and visible features, while crashworthiness was harder to assess before an accident. This reduced the market's ability to consistently reward investments in occupant protection.
- **Uneven adoption of voluntary innovations.** Improvements in restraints and vehicle structures preceded broad regulatory adoption. Their existence did not ensure that every buyer received comparable protection.

Government Intervention as a Turning Point

- **A federal safety framework.** Public advocacy and congressional scrutiny intensified pressure for reform. The National Traffic and Motor Vehicle Safety Act of 1966 established a framework for federal vehicle safety standards [2].

- **Mandated baselines.** Federal standards progressively addressed occupant restraints, safety glass, steering assemblies, head restraints, and other protective functions. These requirements made essential safety performance a shared obligation rather than solely a matter of optional equipment [3].

The Modern Shift: Market Competition for Safety

- **Consumer awareness and crash ratings.** NHTSA's New Car Assessment Program began consumer crash testing in 1979; its five-star rating system followed in 1993. IIHS began issuing crashworthiness ratings in 1995. The programs made aspects of safety performance more visible and easier to compare [3] [4].
- **Safety as a competitive advantage.** Public ratings give manufacturers significant incentives to improve performance beyond minimum requirements. IIHS describes its automobile crashworthiness program as encouraging improvements beyond federal standards and tests [5].

The resulting relationship is mutually reinforcing: regulation establishes *minimum* performance, engineering creates *improved* protections, and comparative evidence helps consumers recognize and reward those improvements.

“Market incentives reinforce the regulatory baseline; they do not replace it.”

4. Comparison of Safety Drivers

Industry	Initial market incentives	Role of government	Modern safety competition
Aviation	Strong incentives to protect passenger trust, avoid aircraft losses, and limit financial exposure. Industry supported early federal standards.	Established common certification, operational, and airspace requirements; coordinated improvements where individual action was insufficient.	Safety remains essential to confidence and viability within a regulated, interconnected aviation operating system.
Automotive	Protection competed with styling, performance, comfort, and price. Voluntary innovations did not ensure universal adoption.	Established minimum safety performance, making essential protection a shared obligation across vehicles.	Public crash ratings make performance visible and encourage improvements beyond minimum requirements.
Cybersecurity	Incentives to protect revenue, reputation, and operations may not capture losses imposed on dependent organizations and the public.	A proposed consequence-based baseline would address essential capability, containment, recovery, and maintained assurance.	Providers can compete on scoped architectural claims, test evidence, bounded compromise, and trustworthy recovery.

5. Is Cybersecurity Fundamentally Different?

Cybersecurity differs in important ways from the historical safety models, but it is not exempt from their engineering lessons. All three domains depend on controlling loss, managing complex interactions, maintaining protection over a life cycle, and demonstrating that safeguards perform as claimed. Aviation and automobiles are themselves increasingly software-dependent systems: a cyber compromise can become a safety failure. The useful distinction is therefore between different conditions of adversity, exposure, and consequence, rather than between unrelated disciplines.

An Adaptive Adversary

Safety engineering addresses faults, human error, environmental stress, and unintended interactions. System security engineering also addresses intentional action by an adversary who can select timing, combine weaknesses, steal legitimate authority, manipulate observations, and attack recovery. Safety programs also consider intentional hazards; adversarial adaptation is nevertheless central to the cybersecurity problem. A successful defensive measure can change the attacker's strategy, requiring assumptions and evidence to be revisited.

Shared Dependencies and Correlated Compromise

A common identity service, cloud platform, software update mechanism, or widely deployed component can link otherwise separate organizations. A compromised dependency can therefore create opportunities for failures across many systems. Aviation and automobiles also face fleet-wide defects and common suppliers. The distinctive cybersecurity concern is that shared software and authority can provide remotely accessible paths for coordinated exploitation and propagation.

Changing Systems and Uncertain Visibility

Software updates, new hardware components, configurations, integrations, delegated authority, and AI tools can change security-relevant behavior after deployment. An incident may involve silent manipulation rather than an immediately visible outage. Restoring availability does not establish that data, commands, identities, and system state are *trustworthy*. The "Adequate Security" article makes the corresponding systems engineering point: adequacy is a maintained judgment that must evolve with mission, threats, dependencies, and evidence [7].

Consequences Beyond the Purchaser

The organization buying or operating a system may bear only part of the harm caused by its compromise. Patients, residents, suppliers, public agencies, and other infrastructure operators may suffer losses without having selected the technology or accepted its risks. This is an economic externality: private purchasing incentives can understate the value of *protection* to society. Safety has similar externalities, but the reach of shared digital services makes the boundary of affected stakeholders especially important.

"A risk accepted by one organization can become a loss imposed on many others."

6. Broad Societal Consequences of Attacked Systems

Computer-system failure under attack is not limited to stolen information or a temporary inconvenience. Digital systems influence physical processes, allocate resources, authenticate authority, coordinate production, and support decisions. Their compromise can remove required system capability, generate unauthorized behavior, or make apparently normal behavior untrustworthy. These are precisely the system-level concerns developed in "Trustworthy Secure Design" [6].

The following are illustrative loss scenarios, not claims that every incident produces these outcomes. The severity depends on the system architecture, operating conditions, duration, geographic scope, available alternatives, and dependencies.

- **Life and health.** Loss or manipulation of clinical systems, medical devices, dispatch services, or water-treatment controls can delay care or create unsafe conditions.
- **Essential services.** Disruption of electricity, water, communications, transportation, or payments can prevent communities from performing ordinary and emergency functions.

- **Economic continuity.** Compromise of logistics, industrial control, settlement, or shared business services can interrupt production and transactions across organizations.
- **Integrity of decisions.** Manipulated sensor readings, records, models, or instructions can cause harmful decisions while services appear available.
- **Public confidence.** Persistent uncertainty about the integrity and recoverability of essential services can weaken confidence in institutions and their ability to protect the public.

An illustrative dependency chain is electricity to telecommunications to logistics to healthcare. A single disruption need not propagate through direct malware transmission: downstream losses can arise because an essential supporting service is unavailable or untrustworthy. Conversely, independent alternatives, protected operating modes, and bounded dependencies can interrupt the chain. Engineering must examine both technical compromise propagation and the propagation of mission consequences.

A Real Case: Change Healthcare, 2024

The February 2024 Change Healthcare ransomware attack demonstrates how compromise of a shared digital service can distribute harm across a sector [11]. In a March 6 memorandum, CMS reported effects across pharmacies, hospitals, and physician offices, including disruption of some people's access to care and prescriptions. CMS also documented interrupted claims submission and Medicare payments and established accelerated and advance payments to help affected providers and suppliers maintain operations [10].

The facts establish disruption beyond the attacked company; the externality interpretation is the analysis advanced here. Providers could have commercial relationships with Change Healthcare, directly or through intermediaries, but affected patients generally did not select the underlying claims-processing service. Their exposure illustrates why the consequences of a digital *dependency* cannot be evaluated solely from the vendor's perspective. The case supports scrutiny of service concentration, viable alternatives, continuity arrangements, and protected recovery; it does not by itself prove which architectural change would have prevented the attack.

7. National and Economic Security Implications

For national security, the concern includes reliable command and control, logistics, defense production, intelligence integrity, and the availability of civilian infrastructure supporting military and emergency operations. An adversary need not destroy a platform to reduce its usefulness. Delayed supply, corrupted instructions, unavailable communications, or uncertainty about trusted state can undermine mission execution.

For economic security, the concern extends beyond incident-response costs. Loss of production, payment capability, logistics coordination, intellectual property, or confidence in shared services can affect firms that were never directly compromised. Concentrated dependencies can magnify disruption; architectures that preserve essential capability and trustworthy recovery can reduce it.

These implications support a *consequence-based* approach to protection. They do not justify treating every application as a national security system. The level of engineering rigor should follow the plausible losses and the importance of the capability being supported. A low-consequence application and a shared service supporting critical national functions require different protection and assurance judgments [6] [7].

"Protection must follow the reach of the loss."

8. Trustworthy Secure Design: Apply the Safety Lesson to Architecture

The strongest connection to safety is the *Security Design Order of Precedence*, established in NIST SP 800-160, Volume 1, Revision 1 [8] and discussed in the “Trustworthy Secure Design” article [6]. It draws on the safety-engineering tradition: eliminate or reduce loss potential through design before relying on additional mechanisms, monitoring, procedures, and training. This ordering gives the historical analogy an engineering foundation.

- **Eliminate through design selection.** Remove unnecessary functions, interfaces, connectivity, privileges, and dependencies that create avoidable loss paths.
- **Reduce through design alteration.** Separate domains, limit shared resources and authority, and structure interactions so one compromised system element cannot readily produce a system-wide loss.
- **Incorporate engineered features or devices.** Provide dependable mediation, enforcement, protected communications, and other mechanisms within the resulting architecture.
- **Provide visibility and feedback.** Detect relevant conditions in time for effective action, while protecting the observations and response functions themselves.
- **Use procedures, training, and equipment.** Support safe operation while recognizing the limits of relying on human action to compensate for structural weakness.

This is a precedence for considering loss-control alternatives, not a prohibition on combining them. Operational cybersecurity remains necessary. Its effectiveness depends on an architecture that limits what an adversary can reach, control, change, and prevent from recovering. Protection functions must also be analyzed for failure, compromise, bypass, and dependency loss [6].

NIST treats security as an *emergent* system property and addresses composition explicitly in SP 800-160, Volume 1 [8]. Individually well-protected components can still compose into uncontrolled information flows, excessive authority, or a shared point of failure. The assurance target must therefore include the complete system and its consequential interactions, rather than only the products deployed within it [6].

9. Adequate Security: Whose Consequences Count?

NIST SP 800-160, Volume 1 defines *adequate security* through two complementary tests, developed further in the “Adequate Security” article: achieve a minimum tolerable security level and make the system as secure as reasonably practicable (ASARP). Crossing the minimum threshold does not automatically justify stopping; further improvements must be evaluated against system objectives and constraints. The resulting judgment requires evidence [7] [8].

For a consequential system, identifying stakeholders is part of establishing that minimum. A company’s tolerance for revenue loss does not establish society’s tolerance for interrupted emergency care, unsafe water, disrupted payments, or degraded national defense. The adequacy argument should explicitly account for affected users, dependent organizations, communities, and public missions.

This broader stakeholder interpretation is a policy and governance implication of the *engineering framework*, not a statement that the cited articles assign a particular government agency authority to set every threshold. Where public consequences are substantial, appropriate public institutions and sector stakeholders should help define the protection needs and tolerability boundaries.

ASARP should likewise be evaluated in a trade space that includes public consequences, rather than only the operator’s direct costs. The framework does not call for unlimited spending or zero risk. It calls for a

defensible explanation of the protection achieved, the improvements considered, the constraints encountered, and the evidence supporting the decision [7].

A Consequence-Based Assurance Claim

An illustrative top-level claim for an essential service is:

Within the defined operating conditions and compromise assumptions, the system maintains the specified minimum essential capability, bounds identified propagation and loss scenarios, and restores an authorized, sufficiently trustworthy state through protected recovery paths.

Supporting evidence should address domain boundaries, privilege allocation, consequential interfaces, shared dependencies, protection-function failure, degraded operation, recovery integrity, and renewed assurance after change. Testing should assume selected components or credentials are hostile and determine whether the system remains within its declared loss bounds. The claim must disclose assumptions and scenarios that exceed the design basis [6] [7].

10. Market Incentives and Public Requirements in the Cyber Era

The historical lesson remains applicable: public requirements can establish a *baseline* while private competition encourages *improvement*. Cybersecurity makes that relationship harder to implement because system boundaries vary, adversaries adapt, and security properties are difficult for buyers to observe. Those difficulties strengthen the need for meaningful evidence rather than making evidence unnecessary.

Technology buyers can readily compare features, price, and performance, but often cannot evaluate the architectural safeguards that prevent and limit loss. This information imbalance can weaken the commercial reward for investing in trustworthy secure design. Providers that omit essential protections may gain a cost or delivery advantage while transferring potential losses to customers, dependent organizations, and the public. Meaningful transparency helps buyers reward stronger engineering; appropriate baseline requirements help ensure that essential protection is not a competitive disadvantage.

“Baseline requirements establish essential protection. Credible evidence makes protection visible. Market competition rewards improvement.”

A Voluntary Race to the Top

Providers can begin by explaining their principal trust relationships, authority boundaries, containment mechanisms, recovery strategies, claim limitations, and supporting evidence. Responsible disclosure need not expose sensitive implementation details. Buyers can make such evidence part of procurement, and providers can compete on demonstrated protection and recoverability as well as features, price, and performance.

A Public Baseline for Consequential Systems

Where failures impose serious costs on others, *voluntary* demand may not establish an adequate floor. A defensible policy approach would emphasize consequence-based requirements, engineering evidence, protected recovery, and reassessment after material change. The details should be tailored to system and sector context rather than reduced to a universal control inventory.

This is a recommendation derived from the comparison, not a claim that aviation certification can simply be transplanted into all software markets. Public crash ratings offer a useful model for making evidence visible,

but no single cyber score can capture every architecture, threat assumption, operational mode, and mission consequence. Comparisons must state their scope, test conditions, limitations, and evidence.

Innovation and Protection Together

Frontier AI can increase defensive capability and the speed and scale of attack, as discussed in “Trustworthy Secure Design” [6]. Its significance is that *architectural* weaknesses may become harder to compensate for operationally. The response should be to integrate protection and assurance into innovation, maintain evidence as systems change, and constrain consequential authority before deploying it broadly.

11. Conclusion

Cybersecurity is different from aviation and automotive safety in its emphasis on adaptive adversaries, remotely exploitable shared dependencies, rapid change, and uncertain system integrity. It shares their central *engineering* obligation: identify unacceptable losses, design to prevent and limit them, and substantiate confidence in the resulting protection.

The broad societal impacts of attacked computer systems make private risk acceptance an incomplete basis for deciding how much protection is enough. National and economic security depend on capabilities whose loss can reach far beyond the purchasing organization. Minimum tolerable security and reasonably practicable improvements must therefore reflect the consequences to all materially affected stakeholders.

The way forward combines trustworthy secure design, maintained adequacy judgments, meaningful transparency, market incentives, and appropriate public requirements. The objective is to make demonstrated protection of essential capability a condition of responsible deployment and a basis for competition.

“Societal dependence makes secure design a national imperative.”

Acknowledgments

The author gratefully acknowledges the support provided by Dartmouth College's Institute for Security, Technology, and Society (ISTS). The resources provided by the ISTS contributed to the research and development of this paper. The views and conclusions expressed herein are those of the author and do not necessarily represent the views of Dartmouth College.

References

- [1] Federal Aviation Administration, "A Brief History of the FAA." https://www.faa.gov/about/history/brief_history
- [2] U.S. Congress, National Traffic and Motor Vehicle Safety Act of 1966, Public Law 89-563, 80 Stat. 718. <https://www.govinfo.gov/app/details/STATUTE-80/STATUTE-80-Pg718>
- [3] National Highway Traffic Safety Administration, "How Vehicle Safety Has Improved Over the Decades." <https://www.nhtsa.gov/how-vehicle-safety-has-improved-over-decades>
- [4] Insurance Institute for Highway Safety, "Who We Are." <https://www.iihs.org/about>
- [5] A. C. Schumacher, E. R. Teoh, and J. M. Nolan, *Lives Saved Through the Insurance Institute for Highway Safety's Crashworthiness Ratings Program*, Insurance Institute for Highway Safety, June 2026. <https://www.iihs.org/research-areas/bibliography/ref/2369>
- [6] R. Ross, "Trustworthy Secure Design: Engineering Security from the Inside Out," RONROSSECURE, LLC, August 2026. SSE Library. <https://ronrossecure.com/library>
- [7] R. Ross, "Adequate Security: An Engineering Answer to an Impossible Question," RONROSSECURE, LLC, August 2026. SSE Library. <https://ronrossecure.com/library>
- [8] R. Ross, M. Winstead, and M. McEvilly, *Engineering Trustworthy Secure Systems*, NIST Special Publication 800-160, Volume 1, Revision 1, National Institute of Standards and Technology, November 2022. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf>
- [9] Federal Aviation Administration, "Lockheed L-1049 Super Constellation and Douglas DC-7," Lessons Learned: Grand Canyon, June 30, 1956. https://www.faa.gov/lessons_learned/transport_airplane/accidents/N6902C
- [10] Centers for Medicare and Medicaid Services, "Addressing Impacts Related to the Cyberattack on Change Healthcare," memorandum, March 6, 2024; and "Change Healthcare/Optum Payment Disruption (CHOPD) Accelerated Payments to Part A Providers and Advance Payments to Part B Suppliers," March 9, 2024. <https://www.cms.gov/files/document/hpmsmemoonchangehealthcarecyberattack03062024.pdf>
<https://www.cms.gov/files/document/hpmsmemoonchangehealthcarecyberattack03062024.pdf>
- [11] U.S. Department of Health and Human Services, "Change Healthcare Cybersecurity Incident Frequently Asked Questions," updated March 14, 2025. <https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html>