Graduate Research Paper

An Integrated Approach to Cybersecurity Governance for Organizations with Established Cybersecurity Programs

Tim Testa

University of Maryland Global Campus

CMAP 635 Cybersecurity Governance

Contents

An Integrated Approach to Cybersecurity Governance for Organizations with Established Cybersecurity Programs

Topic Description

The purpose of this paper is to encourage established organizations (EOs) to reevaluate their current cybersecurity posture while providing clear, practical pathways toward a modernized and more secure cybersecurity governance program. This paper will address common challenges EOs may face when attempting to modernize existing cybersecurity programs (CPs), introduce simplified solutions, evaluate pathways to modernization from multiple starting points, and conclude by examining the question: “Are we protected?”

Introduction

In cybersecurity, the finish line does not keep getting further away; it simply does not exist. Cyber threats change and adapt as quickly as new technologies become available, and the recent boom in Artificial Intelligence (AI) has created new concerns for established organizations (EOs). For that reason, CPs must be designed to be adaptive, resilient, and realistic for the organization’s available resources. This paper will examine the threats EOs face and explain how modern governance practices can help organizations improve cybersecurity management, strengthen mitigation efforts, and better prepare for current and future risks.

The Problem: A Case Study

Most organizations have some form of information technology (IT) department, but the question is whether that department is equipped with the necessary tools and support to prepare for a cybersecurity attack. In 2021, many people in the United States experienced the tangible effects of a cyberattack when Colonial Pipeline became the victim of a ransomware attack. The attack involved a legacy virtual private network (VPN) system that did not have multifactor authentication, allowing access through a password alone (Kelly & Resnick-Ault, 2021). Colonial Pipeline proactively shut down its pipeline system in response to the ransomware attack

on May 7, 2021, and announced on May 13, 2021, that it had restarted its full pipeline system (U.S. Department of Energy, n.d.). The incident also involved a ransom payment connected to the DarkSide ransomware group, and the Department of Justice later announced the seizure of approximately $2.3 million in cryptocurrency proceeds from that payment (U.S. Department of Justice, 2021). Although the pipeline was restored, the incident left the public demanding answers and raised serious concerns about cybersecurity preparedness in critical infrastructure.

Colonial Pipeline, a major fuel pipeline serving the eastern United States, shows how a cybersecurity program can appear functional while still leaving serious gaps. Its cybersecurity program may have checked required boxes, but the incident exposed the difference between basic compliance and a cybersecurity program that is mature enough to withstand a real attack. After this event, several cybersecurity laws, regulations, and mandates followed, eventually contributing to the release of the 2023 National Cybersecurity Strategy (NCS). The NCS emphasized that cybersecurity responsibility should shift toward the organizations most capable and best positioned to reduce cyber risk, rather than relying too heavily on individual users, small organizations, or local governments (The White House, 2023). Since then, C-suite executives have had increasing reason to reevaluate cybersecurity policies and programs to ensure they align with the NCS, CISA, and other regulatory expectations.

Challenges EOs Face When Modernizing Cybersecurity Programs

With new regulatory expectations, laws, and other requirements shaping cybersecurity practices, along with novel technologies and rapidly developing cyberattacks, modernizing CPs has become essential. Unfortunately, companies are often fighting an uphill battle when developing and updating these programs. Some of the most common issues include outdated or complacent cybersecurity policies, human-factor risks being treated as unsolvable, underbudgeted CPs, knowledge gaps, and AI integration.

Negligent or Complacent Cybersecurity Policies

One challenge EOs face is the risk of relying on outdated or complacent cybersecurity policies. Some organizations may be unaware of applicable rules and regulations, while others may assume they are secure because they were compliant several years ago. However, compliance at one point in time does not guarantee continued security. As new technologies

emerge, cyberattacks also become more sophisticated. The rapidly shifting threat landscape means EOs must review and adapt their CPs regularly instead of treating compliance as a one-time achievement. This aligns with the NIST Cybersecurity Framework (CSF) 2.0, which encourages organizations to use cybersecurity outcomes, organizational context, risk, and mission objectives to manage cybersecurity in an ongoing way (National Institute of Standards and Technology [NIST], 2024a).

Human Factors Treated as an Unsolvable Problem

Another challenge is the way organizations approach human-factor risk. One of the most common phrases in cybersecurity program development is that "humans are the weakest link." However, organizations have often treated this risk as unavoidable, relying primarily on annual training instead of implementing stronger mitigation techniques. Verizon's 2024 Data Breach Investigations Report found that more than two-thirds of breaches involved a non-malicious human element, showing why human-factor risk remains a major cybersecurity concern (Verizon, 2024). At the same time, NIST SP 800-50 Rev. 1 supports a more structured learning approach by providing guidance for developing and managing a cybersecurity and privacy learning program as a continuing process rather than a one-time annual task (NIST, 2024b). This means EOs should not treat human behavior as an unsolvable weakness, but as a risk area that can be reduced through better program design, training, and culture.

Convincing the Board

A third challenge EOs often face is the lack of an appropriate budget for an effective cybersecurity program. Cybersecurity technologies and services are not cheap, and a Chief Information Security Officer (CISO) must often justify the budget based on the possibility of a future breach. This relationship between the CISO, decision-makers, and an adequate budget is a fine line. The CISO must explain serious risk scenarios without overselling or catastrophizing, while still emphasizing the importance of being prepared. The upfront costs may be large, but the long-term savings can be significant when compared to the cost of a major cybersecurity incident. IBM's 2024 Cost of a Data Breach research found that organizations with severe security staffing shortages experienced average breach costs that were $1.76 million higher than organizations with low or no staffing shortages, supporting the argument that underinvestment in

cybersecurity personnel and capabilities can carry significant financial consequences (IBM, 2024).

Cybersecurity is still a relatively new and rapidly changing field, which creates many unknowns, uncertainties, and knowledge gaps for established organizations. Like any industry, there are things organizations know, things they do not know, and things they do not yet realize they do not know. These unknowns are common in cybersecurity, but planning for them is difficult because organizations cannot fully prepare for threats they do not yet understand. These uncertainties become even harder to manage when cybersecurity leaders must justify budgets, policies, and modernization efforts without always having tangible evidence of a specific future attack.

Many of these uncertainties are also connected to knowledge gaps among C-suite executives and board members who may have little direct experience with cybersecurity issues. For that reason, decision-makers must surround themselves with competent cybersecurity personnel who can develop strong programs while also educating leadership well enough for them to make informed decisions. Upper leadership knowledge gaps may create challenges during modernization efforts, but leadership buy-in is crucial for cybersecurity governance to succeed. Like most new implementations, modernization of a cybersecurity program will come with complications and friction. There is no viable way to plan for every possible scenario; therefore, cybersecurity professionals must focus on building adaptable programs that can be reviewed, improved, and supported by leadership over time.

Integration of Artificial Intelligence

The recent boom in AI has shifted priorities for industries across the United States and introduced promising developments across many sectors. At the same time, AI has created new threats and vulnerabilities for computer networks. Modernizing cybersecurity programs now allows EOs to adopt AI in a more structured and responsible way. However, before incorporating AI into business operations, organizations must account for both known risks and the many unknown risks that continue to emerge. NIST's AI Risk Management Framework was developed to help manage risks to individuals, organizations, and society associated with AI, which makes it an appropriate guide for EOs considering AI adoption (NIST, 2023). This pressure to

incorporate AI while also managing its risks can become one of the most complicated challenges in modernizing existing CPs.

The Solution: Governance, Risk Management and Compliance

Modernization of CPs has become a priority for established organizations across the nation, and successful modernization introduces the potential for a more secure digital future. While every organization has different risks, resources, and regulatory obligations, effective CPs are typically built on the same foundation: governance, risk management, and compliance (GRC).

GRC: What It Is and How It Impacts Established Organizations

Governance, risk management, and compliance work together as the foundation for a modern cybersecurity program. Governance refers to the act of implementing policies, rules, and procedures to achieve a goal for an organization. In cybersecurity, governance allows cybersecurity professionals to implement policies, rules, regulations, and mandates as tools for improving security and accountability. The first step in modernization is establishing an official cybersecurity program with clearly defined governance. In doing so, cybersecurity becomes a recognized function within an EO, which is key to building a positive cybersecurity culture. Naturally, risk management and compliance work alongside governance to support a well-defined cybersecurity program.

Governance is strongest when it is supported by compliance and risk management. Governance provides the guiding documentation an organization follows to remain compliant. Internal systems should be designed to align with internal governance requirements, while governance principles should also account for business-specific requirements and external laws, regulations, and expectations at the federal, state, and local levels. Failing to comply with industry-specific requirements may expose an organization to legal or regulatory consequences. Compliance with federal, state, and local regulations should not be treated as a checkbox requirement, but rather as part of the foundation from which an organization builds its cybersecurity program.

Risk management complements compliance by helping organizations assess, acknowledge, document, and mitigate cybersecurity risks. The NIST CSF 2.0 supports a proactive risk management approach by helping organizations understand cybersecurity risk and connect cybersecurity practices to organizational goals (NIST, 2024a). NIST, CISA, the Intelligence Community, and other government agencies have produced resources that provide guidance, checklists, and learning materials for EOs seeking to adapt and implement GRC practices. The NIST Risk Management Framework (RMF), for example, provides a structured and flexible process for managing security and privacy risk through categorization, control selection, implementation, assessment, authorization, and continuous monitoring (NIST, 2018). Together, these resources support modernization efforts that are structured, repeatable, and tied to organizational risk.

The Colonial Pipeline breach demonstrates why governance matters. Following the breach, public reporting and testimony showed that a combination of contributing factors, including legacy access and the absence of multifactor authentication on the VPN system involved, increased the organization's exposure to attack (Kelly & Resnick-Ault, 2021). The lesson is not that one control failure explains the entire incident, but that governance should create the oversight, accountability, and review needed to reduce preventable weaknesses. GRC is the foundation of a modern cybersecurity program and is one of the first concepts EOs must target when moving from broad cybersecurity goals to practical modernization efforts.

Governance-Based Solutions to Modernization Challenges

Implementation of governance-based solutions requires effective communication between leadership, boards, department heads, cybersecurity professionals, and other decision-makers, hereafter referred to as "stakeholders." Once modernization efforts are approved, the first step is to identify the appropriate stakeholders and establish clear expectations for communication. Communication is essential to any governance solution and should be treated as both a requirement and a tool. Modernization efforts often do not progress in a perfectly linear fashion, and administrative tasks may need to be prioritized and completed alongside technical controls.

Policy Review and Governance Updates

When updating policies and procedures, EOs should begin at a high level while recognizing that individual policies will eventually need detailed review. The goal is not to rewrite every policy at once, but to improve what already exists while prioritizing critical guiding principles. Policy and guidance review is time-consuming, and that time must be included in modernization planning. NIST CSF 2.0 supports this type of structured approach through the use of Organizational Profiles, which allow organizations to describe current and target cybersecurity outcomes and prioritize improvements based on mission objectives, stakeholder expectations, threats, and requirements (NIST, 2024a).

Policy review should be completed in phases and prioritized by categories such as critical, high, medium, and low. The highest priority should be given to noncompliant policies, especially when those policies relate to industry regulations, federal or state requirements, or contractual obligations. Lower-priority policies may already be compliant, but they should still be reviewed as part of the broader modernization effort. Once priority levels are established, each document should have milestone dates, completion dates, and periodic review dates. Documentation should also have a tracked lifecycle that addresses creation, review, update, cancellation, and expiration. In addition, organizations should identify conflicting policies before releasing new or updated guidance.

Governance should be a primary contributor to modernization efforts because governance gives the organization a way to show that cybersecurity is being managed intentionally. This does not mean governance does not already exist in CPs. Rather, explicitly declaring and organizing GRC efforts provides a clear signal to stakeholders, employees, and clients that cybersecurity is a priority for the organization. Cybersecurity also requires top-down buy-in for an effective and positive cybersecurity culture. C-suite employees and board members have significant influence over organizational priorities, so their messaging must be consistent and clear in its commitment to cybersecurity. This type of leadership support is necessary during modernization because cybersecurity is not only a technical issue; it is an organizational responsibility.

Human-Centered Cybersecurity Training

One of the biggest misnomers in cybersecurity is that humans are the weakest link. It is true that one employee might click a link that allows a hacker to gain access to a computer network, but before that click, there was usually a series of decisions that made the network susceptible in the first place. This is where human-factors research has begun to influence cybersecurity by shifting the focus from blaming individual users to understanding organizational conditions that allow mistakes to become major incidents. This idea also aligns with the NCS principle that national cyber resilience should not depend on one person's constant vigilance or a single user's momentary lapse in judgment (The White House, 2023).

Developing a CP with human factors in mind does not mean the human-factors concern is resolved. Rather, it allows cybersecurity professionals to introduce mitigation techniques with a greater likelihood of success. In years past, annual cybersecurity awareness training was often treated as the default way to address human concerns. Modern trends include phishing simulations, real-world simulations, proactive cybersecurity awareness campaigns, signage, newsletters, and role-specific training. NIST SP 800-50 Rev. 1 supports a lifecycle approach to cybersecurity and privacy learning, which means organizations should design, manage, review, and improve learning programs over time instead of treating training as a one-time compliance requirement (NIST, 2024b). The more cybersecurity and daily operations coexist naturally, the more likely employees are to understand their role in protecting the organization.

Human factors have made strides in the cybersecurity field, but further research and application are still needed. Researchers and practitioners continue to recognize the need for better human-centered cybersecurity practices, but implementation requires funding, leadership support, and time. For EOs, the practical lesson is that human-factor risk should not be treated as an unavoidable weakness. It should be treated as a governance issue that can be reduced through better training, better systems, clearer reporting channels, and a stronger cybersecurity culture.

Risk-Based Budgeting and Executive Buy-In

Hiring cybersecurity professionals, combined with modernization of tools and facilities, is often constrained by budget. Over the past several years, organizations have allocated increasing resources toward securing private networks. While this is a positive trend, budgetary

restraints are always going to exist. If an organization underbudgets its cybersecurity program, the result may be weak controls, delayed modernization, and increased exposure to a breach. If a breach occurs, the organization may also face regulatory enforcement, financial penalties, contractual consequences, and civil litigation depending on the data involved, the industry, and whether the organization failed to maintain reasonable security practices. There is a lot to understand with cybersecurity budgets, and this is where a CISO must become an expert communicator.

Communicating technical considerations to a nontechnical audience seems simple on the surface but must be done with careful precision. Budget proposals often use statistics and data to justify decision-making, but cybersecurity is not so binary. While statistics can show general trends, they do not always reflect the specific risks, structure, or operational changes within a particular organization. For example, an EO that has increased personnel, expanded remote work, adopted new technology, or changed business operations may have a different risk profile than similar organizations in the same industry. This is why the CISO must be able to clearly communicate risk in a way decision-makers understand. The CISO's role is not only to present statistics, but also to explain how those statistics apply to the organization's actual environment and why the requested budget is necessary to reduce risk and adapt with changing technologies. NIST RMF supports this type of decision-making because it provides senior leaders with information needed to make efficient, cost-effective, risk-based decisions about systems supporting the organization's mission and business functions (NIST, 2018).

Responsible Artificial Intelligence Integration

AI is becoming a priority in most industries and shows promise for technological breakthroughs. It can greatly benefit an organization, but it must be used with care and caution. NIST and other agencies have been updating publications to address AI concerns, including risks related to bias, anomalies, reliability, privacy, and misuse. When introducing AI into the workplace, organizations should first understand the risks, known and unknown, and create policies involving safe and legal usage. Enforcing policies is a vital step in AI usage, especially when confidential or protected data is involved.

An EO should not assume that AI tools are appropriate for every type of business information. If an employee uses an AI tool to organize private company matters, that action may

create confidentiality, privacy, contractual, or policy concerns depending on the information involved and the tool being used. AI may also expand the threat landscape by lowering barriers for misuse, accelerating attacker workflows, or creating new risks the organization has not previously documented. The NIST AI RMF supports a structured approach to these concerns by helping organizations manage AI risks to individuals, organizations, and society (NIST, 2023).

An effective approach to mitigating this risk is to build AI policies and training into modernized CPs. AI can be used safely if the knowledge gaps and risks are assessed, understood, and documented. The goal should be to use AI in a governed, documented, and responsible way that supports the organization without creating uncontrolled exposure.

Modernization Simplified: The PAPER Approach

Whether a Fortune 500 company has a fully functional but outdated cybersecurity program, or a small business has one IT employee who handles the Wi-Fi, modernization can be a daunting task. Regardless of the starting point, it is possible. Modernization can be simplified through the acronym PAPER: Plan, Assess, Produce, Execute, and Reevaluate.

Plan

Before modernization efforts can occur, a dedicated amount of time should be allocated to planning. During this phase, lines of communication should be established, milestones and deadlines should be determined, and a list of decision-makers, stakeholders, and affiliated first-, second-, and third-party partners should be aggregated. This may happen before, during, or after budgetary decisions. By the end of this phase, there should be a clear schedule for all required actions moving forward.

Assess

A full assessment of the current cybersecurity posture must be completed before determining actionable steps. This may include anything from a document review to hiring an external penetration testing team to test the network. The assessment phase should be divided among applicable parties and conducted according to the timelines determined in the Plan phase.

Produce

Discoveries made during the Assess phase enable the EO to create a list of actionable items that must be produced. This can include creating new documentation, buying new technology, generating newsletters, or developing training materials. This phase transitions into Execute according to each individual line item.

Execute

Execution includes releasing new or updated documents, replacing technology, conducting new trainings, and implementing other approved changes. This is one of the most critical points in modernization because it is where planning and production become active improvements. Most of the time spent on cybersecurity modernization may occur during the Assess and Produce phases, but executing the plan brings the organization into the final phase: Reevaluate.

Reevaluate

A modernized CP will constantly have new tasks to complete, and with technical and administrative tasks progressing on their own timelines, a cybersecurity professional's work is never truly done. Similar to how policies often have annual or biennial review requirements, all cybersecurity technologies, including physical, logical, and cloud-based systems, should have clearly defined review requirements. This aligns with the NIST RMF because cybersecurity risk management should include ongoing monitoring and review rather than one-time implementation (NIST, 2018). Reevaluate ensures that modernization does not become another one-time effort that eventually turns outdated.

Governance Principles: Laws, Regulations, and Organizational Protection

The PAPER model gives EOs a practical way to modernize, but those efforts must also be guided by the laws, regulations, and industry requirements that apply to the organization. During the Plan and Assess phases, EOs should identify which federal, state, industry-specific, contractual, and international requirements apply to their data, systems, and operations. This matters because cybersecurity failures do not remain purely technical issues. Depending on the organization and the type of data involved, a breach may create legal consequences, compliance

issues, civil lawsuits, fines, and reputational harm. Breach notification laws vary across jurisdictions, but all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring notification when certain personal information is compromised (National Conference of State Legislatures [NCSL], 2022).

Legal and regulatory requirements should also shape how EOs classify and protect data. Organizations must know what data they have, where it is located, who can access it, and what rules apply to it before they can protect it effectively. However, classification alone is not enough. Without governance, defined ownership, and supporting security processes, classification can become a labeling exercise rather than a protection strategy. For that reason, compliance must be connected to practical controls such as access management, encryption, monitoring, incident response, documentation, and lifecycle maintenance.

Governance also protects the organization by making communication and documentation part of the cybersecurity process before an incident occurs. If a breach happens, an EO should already have a process to determine what data was exposed, who was affected, what authorities must be notified, and what records must be preserved. Legal, compliance, cybersecurity, leadership, and communications teams should be involved early so the organization can provide accurate, timely, and consistent information. This aligns with NIST SP 800-61 Rev. 3, which emphasizes incorporating incident response into broader cybersecurity risk management activities (NIST, 2025). Ultimately, laws and regulations should not be treated as a separate checklist outside the cybersecurity program. They should be built into governance documents, policy reviews, training, incident response planning, and documentation practices.

Recommendations for Organizational Leaders

The most important thing organizational leaders can do is stop treating cybersecurity as a purely technical issue. The Cybersecurity and Infrastructure Security Agency (CISA), NIST, and other government agencies provide free guidance, frameworks, and tools that can help EOs modernize their cybersecurity programs (Cybersecurity and Infrastructure Security Agency [CISA], n.d.; NIST, 2024a). Leaders should use those resources, learn from them, and surround themselves with cybersecurity professionals who can translate technical risk into business decisions.

Based on the problems and solutions discussed throughout this paper, organizational leaders should consider the following recommendations:

1. Use NIST and CISA guidance as a foundation for building or updating CPs.
2. Establish GRC ownership and publish transparent cybersecurity efforts.
3. Review existing policies and identify critical tasks.
4. Allocate appropriate funding to CPs.
5. Build human-centered training and AI governance into modernization.
6. Treat modernization as an ongoing effort.

Conclusion

Cybersecurity modernization is not a one-time project. Like any regulated or risk-based program, it must be maintained, reviewed, and updated as threats, technologies, and organizational needs change. Established organizations often already have tools, policies, and resources available, but they may lack the guidance, understanding, or leadership buy-in needed to use them effectively.

Modernization can be accomplished when organizations apply governance principles, take ownership of cybersecurity risk, and develop the knowledge needed to make informed decisions. The answer to “Are we protected?” cannot be a simple yes or no. Cybersecurity is continuous and always changing. While the finish line may not exist, a more secure digital environment is possible when organizations commit to protecting their networks, supporting their cybersecurity professionals, and improving their programs over time.

References

Cybersecurity and Infrastructure Security Agency. (n.d.). *Cross-sector cybersecurity performance goals*. U.S. Department of Homeland Security. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

IBM. (2024). *Cost of a data breach report 2024*. https://www.ibm.com/think/insights/whats-new-2024-cost-of-a-data-breach-report

National Conference of State Legislatures. (2022, January 17). *Security breach notification laws*. https://www.ncsl.org/technology-and-communication/security-breach-notification-laws

National Institute of Standards and Technology. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (NIST Special Publication 800-37 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

National Institute of Standards and Technology. (2024a). *The NIST cybersecurity framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

National Institute of Standards and Technology. (2024b). *Building a cybersecurity and privacy learning program* (NIST Special Publication 800-50 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-50r1

National Institute of Standards and Technology. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST Special Publication 800-61 Rev. 3). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r3

Reuters. (2021, June 8). *Colonial Pipeline CEO tells Senate cyber defenses were compromised ahead of hack*. https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

U.S. Department of Energy. (n.d.). *Colonial Pipeline cyber incident*. https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

U.S. Department of Justice. (2021, June 7). *Department of Justice seizes $2.3 million in cryptocurrency paid to the ransomware extortionists Darkside*. https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

The White House. (2023). *National cybersecurity strategy.* https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Verizon. (2024). *2024 data breach investigations report*. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf