*Proceedings of the IISE Annual Conference & Expo 2023*
*K. Babski-Reeves, B. Eksioglu, D. Hampton, eds.*

# A cybersecurity planning framework for evaluating, selecting, and deploying security controls

**Abstract ID: 3037**

**Laura A. Albert**
**University of Wisconsin-Madison**
**Madison, WI 53706**

## Abstract

Organizations should proactively evaluate and address cybersecurity threats. However, there is not a clear set of guidelines and rules to help organizations make informed decisions surrounding cybersecurity planning. Additionally, cybersecurity practices must keep pace as new threats and technologies emerge. This research seeks to fill this gap by introducing a cybersecurity planning framework composed of three phases that consist of risk assessment, security control selection, and security control deployment. We discuss how risk analysis and integer programming can be used in this framework to help organizations make proactive planning decisions that balance multiple criteria such as risk, cost, and resource utilization.

## Keywords
Cybersecurity Planning; Risk Analysis; Integer programming

## 1. Introduction
Protecting critical cyber-infrastructure requires a layered approach that involves threat identification, the proactive adoption of security controls and defenses, and better response and recovery strategies. Cybersecurity threats are adaptive and persistent, and therefore, defenses must constantly adapt and improve to keep pace with new risks. There is a growing need to protect cyber-physical systems using risk management techniques [1, 2]. However, many organizations find it challenging to keep up with cybersecurity best practices and new defenses given that they operate in resource-constrained environments. Government and industrial standards have been developed to inform planning efforts (e.g., [3 – 5]). These standards provide guidance into security planning, although they cannot be directly used for risk assessment. As a result, many organizations could benefit from the development of analytical tools to support risk-based cybersecurity planning.

In this paper, we introduce a cybersecurity planning framework to help organizations evaluate the security controls they have in place and prioritize additional security controls to implement and deploy. We take a high-level systems perspective to provide insight and guidance into the overall process. The framework we introduce supports risk-based decision-making using an organization's limited resources, and it supports proactive planning, not real-time detection, response, or recovery. The framework is composed of three phases that consist of risk assessment, security control selection, and deployment. In the first phase, we utilize a questionnaire, with questions developed in conjunction with experts in industry corresponding to security controls used for a specific industry. We develop a scoring mechanism based on risk analysis to evaluate an organization's questionnaire answers to inform risk planning decisions. Then, we outline how methods based on integer programming can identify a set of additional security controls to adopt, and we discuss how an organization can deploy the selected security controls. The questionnaire and the scores were developed with input from subject matter experts (SMEs) from industry who support the commercial real estate sector, and the approach can be the basis for other markets.

This paper is organized as follows. In Section 2, we introduce and overview the cybersecurity planning framework. Section 3 introduces the risk assessment questionnaire and its scoring mechanism. Section 4 investigates how to recommend security controls to manage risk, and Section 5 describes how to manage the phased roll-out of security controls. In Section 6, we offer concluding comments.

## 2. Cybersecurity Planning Framework

In this section, we overview phases of a cybersecurity planning framework to help organizations assess risk and select security controls to protect against a variety of threats. Cybersecurity planning falls into the "Protect" function in NIST's Cybersecurity framework [2]. The functions—identify, protect, detect, respond, and recover—organize basic cybersecurity activities at their highest level. The "Protect" function captures the selection and deployment of cybersecurity safeguards to limit or contain the impact of a potential event, and it is composed of several phases. Our framework focuses on three phases related to planning: (1) risk assessment, (2) security control selection, and (3) deployment. Figure 1 provides a schematic of the three phases in the cybersecurity planning framework. Next, we briefly introduce these three phases.

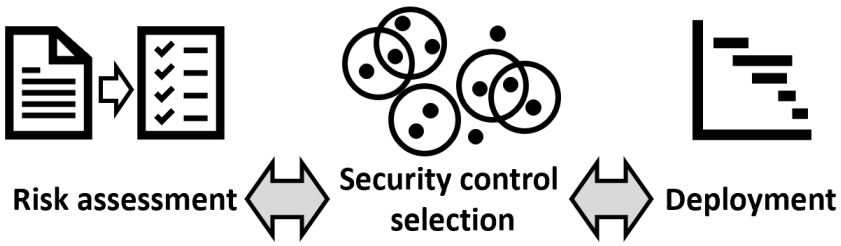


**Figure 1:** Cybersecurity planning framework schematic

### 2.1. Risk assessment

There are several government and industrial cybersecurity standards that are used to guide planning decisions (e.g., [3 – 5]). Over time, many organizations have adopted these standards as mandatory controls. However, cybersecurity standards were not developed as risk management tools, and compliance with standards does not necessarily equate to risk-reduction. In addition, complying with all standards is resource-intensive for most organizations, which can deplete organizations' limited security resources [6]. There is a need to understand how various security controls can reduce risk so organizations can prioritize security controls in a sustainable way as well as balance risk reduction with other criteria, such as cost and resource utilization. Risk assessments to support cost-effective cybersecurity decision-making have met limited success due to the challenges in assessing risk [7, 8], accounting for human behavior [8], and deploying security controls in resource-constrained environments [6].

In recent years there has been increased interest in risk-based approaches to support cybersecurity planning [7, 9]. Evaluating risk involves identifying potential threats (vulnerabilities), estimating the conditional probability that each vulnerability is exploited, and identifying the expected consequences [1, 9]. Risk assessments rely on subject matter expert (SME) elicitation and subjective risk assessments. In industry, extensive questionnaires are often given to owners, vendors, integrators, and others who construct cyber defenses. The questionnaires are designed to proactively address cybersecurity issues by performing security risk assessments, although there are no industry-wide standard questionnaires that would allow for a more efficient use of SME time and consistent risk assessments.

### 2.2. Security control selection

There is a growing body of literature that studies how to mitigate cybersecurity risk through the strategic prioritization of security controls [9]. Enayaty-Ahanger et al. [10] provide a survey of optimization models for cyber-infrastructure security, including research that informs planning decisions. They note the importance of employing analytical tools to shed light on how to use limited resources to inform risk-based planning decisions in resource-constrained settings. A simple approach is to estimate the risk reduction associated with a security control and to prioritize security controls in rank order based on their cost-effectiveness [9]. More sophisticated approaches prioritize the selection of security controls by considering factors such as cost, overlapping capabilities, uncertainty in security control effectiveness, and the role of adaptive adversaries [11 – 13]. Attack modeling is important for cybersecurity protection models. Attack modeling often utilizes attack graphs to characterize potential attacks, where each path represents a series of exploits to achieve attack goals. Zheng et al. [11] introduce integer and stochastic programming models to select a portfolio of security controls subject to a security budget based on the linkages between the security controls and exploits in a set of attack graphs. This model was extended to consider two objectives, the first that maximizes the overall risk reduction and the second that maximizes the weighted number of attacks secured past a risk threshold [12]. Other research studies how to select a cost-effective set of security controls that maximally delay adversarial

attacks that are attempted by multiple adversaries, given that there is uncertainty regarding how effective security controls may be [13].

### 2.3. Deployment

When new security controls are developed, they need to be implemented and operationalized in a timely manner by security personnel. However, there is a dearth of literature considering this issue despite its importance for achieving high levels of security. The importance of deployment is illustrated by the Equifax breach that was caused by the vulnerability Apache Struts CVE-2017-5638 in 2017 [14]. A patch for the vulnerability was released on March 7, 2017, but Equifax left the vulnerability unpatched until July 29, 2017 [14]. It later became evident that Equifax's IT systems had been breached and that the sensitive, personal data of 148 million of their customers had been exposed. The Equifax breach highlights the need for the phased roll-out of security controls, since merely having a patch to address a critical vulnerability is not adequate for protecting critical systems. To effectively manage risk, organizations need to deploy security controls, such as patches, and inform how security personnel incorporate these protection strategies into employee workflows. However, recent industry surveys indicate that deploying security controls is resource intensive [6], and resource limitations can delay or prevent security controls from being implemented. These issues have not yet been adequately addressed in the literature. Doing so would lift the assumptions made in the security control selection phase that security controls are either deployed or not deployed (a binary decision) and that these decisions are made in a single time period. Instead, deployment would inform the choice and implementation of security procedures, including how to deploy security controls. Optimal deployment, as opposed to ad hoc deployment, can match resources to risk, thereby offering the potential to reduce risk without increasing cost.

In the following three sections, we describe how analytical methods drawing upon risk analysis and integer programming can help guide the assessment, selection, and deployment of security controls.

## 3. Risk Assessment Questionnaire

We describe a risk assessment questionnaire scoring mechanism developed in conjunction with SMEs from industry. The questionnaire was developed to provide a consistent set of rules and guidelines for cybersecurity planning in the commercial real estate industry from a third party. This industry was used for proof-of-concept, with the idea that the questionnaire could be adapted to serve as the basis for a risk assessment for other markets. The questionnaire was motivated by the need for organizations to efficiently identify and manage cybersecurity risk. The vendors of products connected to building systems frequently fill out product questionnaires to assess security risk and to inform planning decisions. The questionnaires have similarities, but are phrased and scored differently, leading to inconsistent feedback. The questionnaires are also time-consuming and burden organizations. The overall goal of a standard questionnaire implemented by a third party is to improve cybersecurity standards in a way that helps organizations better manage risk by providing consistent and regular feedback.

In the questionnaire, security controls were considered across 11 categories of protection that are non-overlapping and complete. This allows us to assume independence across multiple categories of protection when assessing risk. The questionnaire consists of a total of 295 questions across the 11 categories, each of which corresponds to a single security control and its implementation. A total of 226 questions (76.6% of the total) require yes/no responses to simplify the implementation, with a “yes” response corresponding to a best practice, typically based on government or industrial standards [3 – 5]. Of the remaining questions, 57 questions (19.3% of the total) are multiple choice and 12 are free form (4.1% of the total). The multiple choice questions correspond to different types of implementation of a security control. Examples include how frequently passwords must be updated or how long video footage is saved.

Our main contribution is a scoring mechanism for the questionnaire. Performing a risk assessment is particularly challenging when implementing a questionnaire across multiple organizations. We could not directly estimate distributions for conditional probabilities and consequences, since those would be organization and setting specific. Instead, we adopted a simplified process that scores each question more generally based on typical implementations of security controls in the commercial real estate industry. We initially assumed each security control is independent to assess risk in an additive way. This assumption is lifted for security control selection in Section 4. Then, we elicited a weight for each question from three cybersecurity SMEs from industry. The weight for each question reflects the reduction in the expected consequences of a successful attack associated with each security control, where the weight approximately captures the reduction in risk (the change in the product of the conditional probability of success and expected consequences) for a typical organization. The three SMEs initially identified three tiers of weights: *preferred*, *urgent*, and *critical*. Further analysis indicated a need for an additional tier: *super-critical*. Weights were elicited for

these four tiers, and these weights were refined after evaluating sample questionnaire answers. The final weights are 1 = *preferred*, 2 = *urgent*, and 5 = *critical,* and 10 = *super-critical*. Note that the weights and the assignment of weights to questions might differ for other markets.

SME elicitation was used to score the answer to each question. All yes-no questions (76.6% of all questions) were given a value of 0 for a no answer and 1 for a yes answer, and other questions (23.4% of all questions) were scored based on SME input to take on values between 0 and 1 based on the proportion of risk reduction that the particular security control implementation would achieve. We provide a summary of the questions that inform the risk assessment.

The questionnaire is scored by summing the points for the questions in each category, weighing the point total by the category weight, and then summing the weighted points in each category. Each category was initially assigned a category weight of 1 to quantify the impact of each question equally. Later, the SMEs recognized a need to re-weigh the categories to account for the different number of questions (security controls) in each category. To achieve this, three SMEs first estimated the total fraction of risk addressed by the security controls in aggregate in each category (these values added to 1.0). These values were rescaled based on the total number of points associated with the questions in each category to yield the (unscaled) category weights. The category weights were scaled such that the total number of points is between 0 and 100, with 100 being the ideal score.

Table 1 summarizes the questionnaire and its scores. It reports the scaled category weights, the distribution of the number of questions in each category across the four tiers, and the total weighted points in each category. The questionnaire yields scores in each category as well as an overall score to communicate risk to the organization that completes it. Additionally, alternative questionnaires could be developed for different stakeholders, such as owners, vendors, and integrators, to reflect their responsibility in managing risk.

**Table 1:** Questionnaire summary

| Category | Category weight | Number of questions in each tier | | | | Number of questions | Total weighted points |
|---|---|---|---|---|---|---|---|
| | | Preferred | Urgent | Critical | Super Critical | | |
| Company information | **0.40** | 0 | 5 | 0 | 0 | **5** | **4** |
| Physical Security | **0.06** | 0 | 2 | 11 | 5 | **18** | **6.5** |
| Network Topology | **0.08** | 2 | 13 | 11 | 4 | **30** | **10** |
| Authenticate & Admin | **0.05** | 7 | 1 | 27 | 7 | **42** | **11** |
| Remote Access, Mobility | **0.09** | 8 | 12 | 2 | 4 | **26** | **7.25** |
| System Endpoint | **0.11** | 3 | 14 | 9 | 2 | **28** | **10.5** |
| Data Center | **0.06** | 2 | 6 | 22 | 3 | **33** | **9** |
| Vulnerability Management | **0.10** | 4 | 1 | 11 | 3 | **19** | **9** |
| Data Storage | **0.07** | 5 | 20 | 11 | 2 | **38** | **8.5** |
| Policies | **0.16** | 1 | 2 | 5 | 4 | **12** | **11** |
| Bus Continuity | **0.05** | 7 | 6 | 17 | 5 | **35** | **7.75** |
| Training | **0.61** | 9 | 0 | 0 | 0 | **9** | **5.5** |
| **Total** | | | | | | **295** | **100** |

In the following two sections, we overview how industrial engineering methods based on integer programming could use the questionnaire results to select and deploy security controls.

## 4. Security Control Selection

The questionnaire score evaluates a portfolio of security controls. If this portfolio is inadequate for managing risk, a remediation plan can recommend security controls to adopt to reach an acceptable risk score. In this section, we outline how models from the literature can inform the selection of a set of security controls that is cost-effective and maximizes risk reduction. One simple way to create a remediation plan is to recommend the adoption of all security controls above a certain level (e.g., all *critical* and *super-critical* controls) at their highest levels. However, this

approach is based on compliance and not risk analysis, and as a result, it may over-burden already resource-constrained organizations and may not lead to implementations that reduce actual risk to acceptable levels. To overcome these limitations, we recommend approaches based on integer programming and risk analysis.

Previous research on budgeted maximal multiple coverage models [11] introduces new integer and stochastic programming models to maximize overall risk reduction under uncertainty subject to a security budget. They account for dependencies between security controls by including multiple choice constraints and by modeling how security controls map to specific vulnerabilities in attack graphs. We propose adapting the modeling approach by [11] to use in conjunction with questionnaires. First, a mapping of questions from the questionnaire to security control standards can capture the dependencies between security controls, which in turn can be used as inputs for the integer programming model. The objective in [11] seeks to maximize overall risk reduction, not how to systematically reduce risk to an acceptable level for as many potential attacks as possible. This objective can be trivially adapted to identify a minimum cost set of security controls to reach a pre-specified overall questionnaire score (i.e., risk level).

Another approach is to prioritize security controls in such a way that an acceptable score is achieved in each questionnaire category. To do so, we can adapt the model the approach by Schmidt et al. [12] who introduce a bi-objective integer programming model that balances overall risk reduction (the same objective as in [11]) with a second objective that seeks to maximize the (weighted) number vulnerabilities whose risk levels are past an acceptable level as defined by a risk threshold. This second goal can be used to identify a cost-effective set of security controls to achieve an acceptable level in each category. For example, the analysis may recommend switching from a SMS-based multi-factor authentication (MFA) to MFA using an authentication app as one of the security controls.

## 5. Deployment

We recognize that selecting security controls is not sufficient for risk management—the security controls must be deployed. The problem of how to effectively implement a phased roll-out of security procedures remains an open problem in the literature. Rather than simply deciding which security controls to implement (a series of binary decisions), a phased roll-out of security controls dictates how limited resources are used to implement these controls over time. The resources can correspond to personnel time (with different types of personnel) and security budgets over deployment time horizons. For example, implementing MFA using an authentication app consists of selecting a vendor, checking compliance requirements, planning for a variety of access needs, educating users, distributing an app, implementing the new requirement, and responding to alerts over an extended time horizon. Without a deployment plan that takes limited resources into account, the proposed security controls may not be feasible with respect to an organization's resources, which in turn may prevent some security controls from being implemented. This could undermine planning efforts and lead to an organization accepting higher than anticipated levels of risk.

To support deployment decision-making, we propose a new approach that draws upon integer programming models in the scheduling literature to deploy security controls across multiple time periods. One approach is to model this problem as an extension of the Resource Constrained Project Scheduling Problem (RCPSP) [15]. Traditionally, the RCPSP seeks to schedule a set of *jobs* (security controls) with an objective that minimizes the makespan of the project. Each job requires resources of different types for deployment, and there may be precedence relationships between jobs. The RCPSP could use the output from the security control selection phase (see Section 4) as an input. The RCPSP is a well-studied problem in the literature with several variants. One such variant to consider is the multi-mode RCPSP (MRCPSP), where each job can be completed in one of several *modes*, which provide alternate resource/duration options for each job [15]. In the deployment domain, this may reflect different deployments of the same security control from different vendors or different implementations of the control that may reflect how often a task must be performed (e.g., every 30 days versus every 180 days). The output of this modeling approach could identify different security control implementation patterns and provide for the flexibility in the scheduling out of each control by dividing each control into a sequence of jobs to be completed.

## 6. Conclusions

Protecting cyber-physical systems against dynamic threats in resource-constrained systems requires analytical tools to support risk management and decision-making. This research recognizes that risk assessment ultimately requires a detailed plan that may require multiple phases. We take a systems approach and outline three such phases: risk assessment, security control selection, and deployment. A risk assessment can be used to identify areas where additional protection is required. Security control selection prioritizes solutions to help manage risk, and deployment

helps the selected security controls be rolled out over time. When these phases are coordinated, they can be used to construct effective security defenses using limited security resources.

We recognize the opportunity to use industrial engineering methods drawing from risk analysis and integer programming to support decision making across all three phases in the cybersecurity planning framework. However, there are other possible approaches that could be utilized. Other aspects of cybersecurity—including detection, response, and recovery—could benefit from robust study using industrial engineering principles to give decision-makers a suite of tools to use for proactive planning.

## Acknowledgements

This work was funded by the National Science Foundation Award 2000986. The views and conclusions contained in this document are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the National Science Foundation. The author would like to gratefully acknowledge David Bunzel, Min Kyriannis, and two other anonymous industry experts for their input and feedback.

## References

[1] The White House, "Executive Order on Securing the Information and Communications Technology and Services Supply," Office of the Press Secretary, Washington, D.C., 2019.

[2] National Institute of Standards and Technology (NIST). "Framework for improving critical infrastructure cybersecurity," version 1.1. Technical report, NIST, Washington, D.C., 2018.

[3] National Institute of Standards and Technology (NIST). "Security and privacy controls for federal information systems and organizations," NIST Special Publication 800-53, Revision 4, Washington, D.C., 2013.

[4] R. Ross, V. Pillitteri, K. Dempsey, M. Riddle, G, Guissanie. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," National Institute of Standards and Technology Report SP 800-171 Rev. 2, Washington, D.C., 2020.

[5] The Center for Internet Security. "The CIS Critical Security Controls for Effective Cyber Defense," Version 6.0, East Greenbush, NY, USA, October 15, 2015.

[6] R. Stevens, J. Dykstra, W. Knox Everette, J. Chapman, G. Bladow, A. Farmer, K. Halliday, and M.L. Mazurek. "Compliance Cautions: Investigating Security Issues Associated with US Digital-Security Standards," in *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium*, San Diego, CA, USA, February 23-26, 2020, doi: 10.14722/ndss.2020.24003.

[7] G. D. Wyss, J. F. Clem, J. L. Darby, K. Dunphy-Guzman, J. P. Hinton and K. W. Mitchiner, "Risk-based cost-benefit analysis for security assessment problems," in *Proceedings of the 44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, San Jose, CA, USA, October 5-8, 2010, pp. 286-295, doi: 10.1109/CCST.2010.5678687.

[8] N.M. Scala, A.C., Reilly, P.L. Goethals, M. Cukier. "Risk and the five hard problems of cybersecurity," *Risk Analysis*, vol. 39, no. 10, pp. 2119-2126, 2019, doi: 10.1111/risa.13309.

[9] D.W. Hubbard, and R. Seiersen. *How to measure anything in cybersecurity risk*. Hoboke, NJ, USA: John Wiley & Sons, 2016.

[10] F. Enayaty-Ahangar, L.A. Albert, E. DuBois, "A survey of optimization models and methods for cyberinfrastructure security." *IISE Transactions*, vol. 53, no. 2, pp. 182-198, 2020, doi: 10.1080/24725854.2020.1781306.

[11] K. Zheng, L.A. Albert, J.R. Luedtke, E. Towle, "A budgeted maximum multiple coverage model for cybersecurity planning and management." *IISE Transactions*, vol. *51, no.* 12, pp. 1303-1317, 2019, doi: 10.1080/24725854.2019.1584832.

[12] A. Schmidt, L.A. Albert, K. Zheng. "Risk management for cyber-infrastructure protection: A bi-objective integer programming approach," *Reliability Engineering & System Safety*, vol. 205, 2021, no. 1, pp. 107093, 205, doi: 10.1016/j.ress.2020.107093.

[13] K. Zheng, L.A. Albert. "Interdiction models for delaying adversarial attacks against critical information technology infrastructure." *Naval Research Logistics,* vol. 66, no. 5, pp. 411-429, 2019, doi: 10.1002/nav.21859.

[14] Electionic Privacy Information Center (EPIC), "Equifax data breach," website, 2022. [Online]. Available: https://archive.epic.org/privacy/data-breach/equifax/ [Accessed December 15, 2022].

[15] Kolisch, Rainer, Arno Sprecher, and Andreas Drexl. "Characterization and generation of a general class of resource-constrained project scheduling problems," *Management science*, vol. 41, no. 10, pp. 1693-1703, 1995, doi: 10.1287/mnsc.41.10.1693.