Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management

NICOLE RADZIWILL AND MORGAN BENTON

There is no standard yet for measuring and controlling the costs associated with implementing cybersecurity programs. To advance research and practice toward this end, the authors develop a mapping using the well-known concept of quality costs and the framework core within the cybersecurity framework produced by the National Institute of Standards and Technology (NIST) in response to the Cybersecurity Enhancement Act of 2014. This mapping can be easily adopted by organizations that are already using the NIST cybersecurity framework (CSF) for cybersecurity risk management to plan, manage, and continually improve cybersecurity operations. If an organization is not using the NIST CSF, this mapping may still be useful for linking elements in accounting systems that are associated with cybersecurity operations and risk management to a quality cost model.

KEY WORDS

cost of quality, cyberquality, cybersecurity, cybersecurity standards, quality costs, risk management

INTRODUCTION

In 1995, ASQ presented an article in its flagship publication *Quality Progress* about “cyberquality,” defined as “information about quality you can find on the Internet” (Clauson 1995). Because technology has progressed by orders of magnitude over the past two decades, this use of the term now seems overly simplistic. There is a new cyberquality, which is readily apparent in the ISO 9001 definition of quality: “the totality of characteristics of an entity that bear upon its ability to satisfy stated and implied needs.” If that entity is a networked, connected device or system, then the stated and implied needs of customers and other stakeholders cannot be met without cybersecurity.

With the growth and evolution of the internet of things (IoT), people, vehicles, homes, city infrastructures, and industrial infrastructures are becoming more tightly interconnected, requiring new strategies for designing quality into systems (Radziwill and Benton 2017). At the same time, there is a need for more robust metrics for controlling and continuously reducing the costs associated with both quality assurance and cybersecurity risk management. Cyberquality will become the net effect of simultaneously meeting quality goals and cybersecurity goals, so it makes sense to explore cost metrics that are linked to both domains.

As the number of networked components increases, so does the potential for catastrophic impact. Over the last several years, reports of software deployed over the internet designed to destroy infrastructure have increased—and infrastructure impacts all organizations. Such "cyberattacks" typically occur when software is deployed, usually (but not always) via a network, onto other systems with the intent of destroying physical or information assets (for example, the Stuxnet case; see Farwell and Rohozinski 2011). These attacks occur via a number of attack vectors, and not all are technological; systems can also be breached maliciously or accidentally by insiders, and social engineering can be used to trick trusted users into giving up their passwords or answers to security questions. With nearly 26 million IoT endpoints expected by the year 2019, the pace and intensity of intrusions will increase (Trautman and Ormerod 2017).

Because "repeated cyber intrusions into critical infrastructure [demonstrated] the need," in 2013, President Obama issued Executive Order 13636 (EO 13636) directing the National Institute of Standards and Technology (NIST) to create a "framework to reduce cyber risks to critical infrastructure" (Obama 2013, 11739). In the context of this order, "critical infrastructure" refers to:

> "… systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." (Obama 2013, 11739)

This article explores the intersection of the NIST Cybersecurity Framework (CSF) and quality cost models, with the goal of making it easier for organizations to study, monitor, and control the costs associated with cybersecurity. Although the NIST CSF was intended to support the critical infrastructure systems that most production systems rely on, it is broadly applicable for cybersecurity risk management at organizations of all sizes.

BACKGROUND

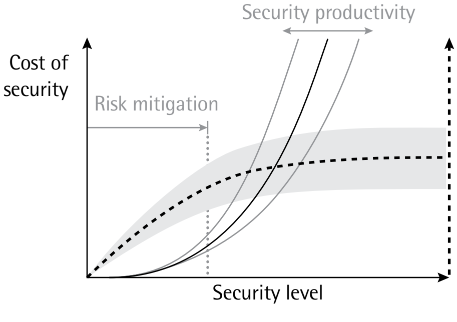
There are four topics that inform the mapping that serves as the primary contribution of this article. They are: cybersecurity economics, the NIST CSF, the concept of quality costs, and models that describe how quality costs are typically distributed in organizations. These topics are covered in order in the following sections.

Cybersecurity Economics

Protecting the confidentiality, integrity, and accessibility of information takes time, effort, and money. Research on the costs of cybersecurity dates back nearly two decades, mostly focused on two themes: budgeting appropriately and determining the economic impacts of cyberattacks. For example, Campbell et al. (2003) examined the economic implications of cybersecurity breaches using stock market performance as an indicator. By creating models that estimated the stock valuation in the absence of an attack, and comparing them to stock performance after attacks, they found detectable dips in stock price only following attacks that involved unauthorized access to confidential data. Attacks that did not appear to have a direct impact on the customer were not associated with this same pattern.

Böhme (2010) performed a comprehensive review of the literature to examine relationships between the costs of information security and benefits realized from making those expenditures. Böhme recognized that there is a baseline level of security provided by preventive efforts for risk mitigation, along with testing those elements. At some point, the costs level out (as shown in Figure 1), so to provide robust mitigation of external breaches, it would cost much more than many organizations are willing to invest. There is "art and

FIGURE 1 Cost/Benefit relationships in information security (Böhme 2010)



©2017, ASQ

science" associated with identifying the ideal balance, so the author recommends using return on security investment, which is the benefits less the costs, divided by the costs, and converted into a percentage.

Brecht and Nowey (2013) reviewed all techniques that had been applied to assessing the costs of information security and categorized them into four areas: cost/benefit analysis of cybersecurity (including research on optimal investment), cost of cybercrime, surveys summarizing the actual costs of cybersecurity management, and quality cost models. The category on quality cost models was the only one that did not cite research directly related to the domain of information security, but rather seemed to suggest that applying quality cost models would be a logical next step. They suggest that effective cost models in cybersecurity will address the costs of purchasing, operating, implementing, and depreciating tools and systems; costs of operating those tools and systems; costs of consulting or other labor; and cost of risk or uncertainty.

Gordon, Loeb, and Zhou (2011) examined the impact of cyberattacks on stock returns and found that when grouped according to the three tenets of information security (that is, confidentiality, integrity, and availability), breaches that impact availability have the greatest negative effects. Gordon et al. (2015) extended the Gordon-Loeb (GL) model for determining the optimal level of investment in cybersecurity activities to account for externalities such as botnets (global networks of infected computers that can be used to launch denial of service attacks, or compromised individuals who engage in psychological warfare on behalf of a nation-state, terrorist, or activist group). With externalities considered, they found that most organizations underinvest in cybersecurity operations, and affirm that "governments around the world are justified in considering regulations and/or incentives designed to increase cybersecurity investments by private sector firms."

Moore, Dynes, and Chang (2016) interviewed 40 executives with primary responsibility for cybersecurity, selected from chief information security officers and chief information officers drawn mainly from healthcare, financial, retail, and government. Thirty-one of the respondents were from the United States, and none were international. The questions, which were exploratory in nature, focused on how threats were identified, prioritized, and managed, and the decision-making process for cybersecurity investments at the respondents' organizations. They noticed few differences among the industry sectors and remarked that finding qualified cybersecurity professionals seemed, in general, to be much more challenging than finding funding to support cybersecurity.

These authors also drew a conclusion that is directly relevant to the need for the present study. They report that in practice, "there is much less focus on the actual results of cybersecurity efforts, such as examining costs and the effectiveness of controls. This may be due to the widespread use of frameworks [such as the NIST Cybersecurity Framework], which promote the use of process measures." A mechanism for examining costs that is aligned with a process-based framework thus may have rather broad applicability.

The NIST Cybersecurity Framework

The Cybersecurity Enhancement Act of 2014 further clarified the intent of EO 13636, directing NIST to "facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure" (S.1353 2014). Responding to this charge, NIST published three requests for information to learn how organizations were managing cybersecurity risk, and to identify best practices. NIST published its first version of the CSF, which captured and organized the results, in February 2014.

The NIST CSF provides proactive risk-based guidance and a common, technology-neutral language for cybersecurity management. It complements an organization's cybersecurity operations, can be used to launch a cybersecurity program where none exists, and can be used in conjunction with other standards and guidance, including ISO 31000 (Risk Management), the ISO/IEC 27000 series (Information Security Management Systems), and NIST Special Publication (SP) 800-39 (Managing Information Security Risk). Although designed with the protection of critical infrastructure (power generation, water/wastewater management, transportation systems) in mind, it can be applied to manage cybersecurity risk in any environment. The framework is voluntary, not prescriptive, and can be used with many different risk management tools, techniques, and practices.

NIST CSF is a toolkit of 98 "pointers" to guidance provided by five standards or collections of best practices. The pointers, called subcategories, are classified into five functions: identify, protect, detect, respond, and recover. The five functions are further broken down by tasks in cybersecurity risk management, which are referred to as categories. The table of functions, categories, subcategories, and informative references is called the framework core.

Figure 2 shows how the framework core begins. The first category, "asset management," contains six of the 98 total subcategories (pointers to the standards and guidance are in the far right column). Each subcategory represents an objective, task, or group of tasks that must be performed to advance cybersecurity risk management. For example, ID.AM-1 is "Physical devices and systems within the organization are inventoried." This specifies *what* must be done, not *how* it should be done. The "informative references" column on the far right directs the NIST CSF user to applicable areas of standards and guidance that could be considered as the organization is deciding *how* to inventory devices and systems.

There are five standards/guidances that are leveraged by the NIST CSF. Together, they provide a comprehensive platform for unified cybersecurity operations, risk management, and strategic management. These are:

- **Center for Cybersecurity Top 20 Critical Security Controls (CCS CSC)** – A standard for computer security that outlines 20 key actions that can be taken to block or mitigate the effects of known attacks (CIS 2013). The 20 controls have been mapped to the five NIST CSF functions (SANS 2016).
- **COBIT 5 (ISACA 2012)** – A business framework for management and governance

FIGURE 2 The first category (asset management) in the framework core (NIST 2014b)

Category	Subcategory	Informative References
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
	ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
	ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
	ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholder (e.g., suppliers, customers, partners) are established.	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1 • **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

©2017, ASQ

of information security. It is used to translate business and customer-focused needs into actionable operations objectives.

- **ISA/IEC 62443-2-1:2009/ISA 62443-3-3:2013 (ISA/IEC 2013)** – Standards specifically for the security of industrial control systems, formerly known as ISA99.
- **ISO/IEC 27001:2013 (ISO/IEC 2016)** – Standards describing best practices for the management of information security, and also providing a path toward compliance with HIPAA, Sarbanes-Oxley, and payment card industry (PCI) regulations.
- **NIST Special Publication (SP) 800-53 Rev. 4 (NIST 2013)** – Security controls and assessment procedures organized into 18 groups, each with its own specific function (for example, access control, contingency planning, incident response)

An alternative view of the framework core is also available (NIST 2014c). Shown in Figure 3, this mapping provides the same information as in the framework core, but no descriptions are provided and there is a separate column for each reference. This supplement is useful for organizations that already have institutional capabilities aligned with one or more of the references, and do not plan to consult every one. The coverage of subcategories is also clearer in the alternative mapping of the framework core than it is in NIST (2014b).

The NIST CSF links strategic planning, quality management, risk management (for example, using ISO 31000), and cybersecurity operations (see Figure 4 on the next page). Because it fills the gap between cybersecurity operations and the quality/risk planning efforts that are usually only done at the executive and business process levels, it plays a central role in other tools and frameworks. This includes the Baldrige Cybersecurity Excellence Builder (BCEB), and the widely applied Cybersecurity Capability Maturity Model (C2M2) family for domain-specific assessment and continuous improvement of cybersecurity risk management. C2M2 guidance covers electric power generation and distribution, oil/natural gas, and dams (Miron and Muita 2014).

Quality Cost Models

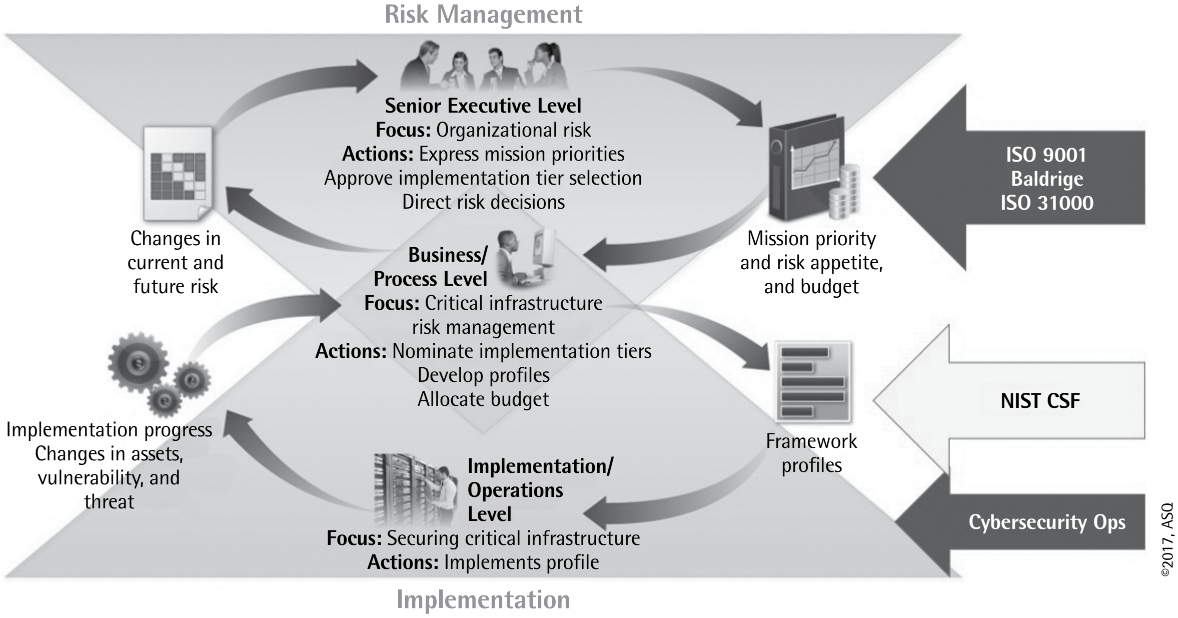
Quality is often promoted as a key element for achieving and maintaining competitiveness, and cost of quality (CoQ) metrics can be used to facilitate quality improvements that translate into cost reductions (Campanella 1999a; 1999b). This concept has been applied to manufacturing tangible products, software-intensive products and systems, and components in the IoT, and can be applied in both development and operations contexts (Radziwill 2006).

There are many variations on quality cost models (sometimes referred to as "cost of poor quality") in the literature. All models address the cost of conforming to requirements and the cost of failing to conform to those requirements; some even include opportunity costs (the costs associated with not taking a certain action) (Schiffauerova and Thomson 2006). The most commonly used models establish that the *cost of*

FIGURE 3 Alternative mapping of the framework core (NIST 2014c)

Function	Category	Subcategory	CCS CSC	COBIT 5	ISA 62443-2-1 :2009	ISA 62443-3-3 :2013	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4
ID	AM	AM-1	CSC 1	BAI09.01, BAI09.02	4.2.3.4	SR 7.8	A.8.1.1, A.8.1.2	CM-8
ID	AM	AM-2	CSC 2	BAI09.01, BAI09.02, BAI09.05	4.2.3.4	SR 7.8	A.8.1.1, A.8.1.2	CM-8
ID	AM	AM-3	CSC 1	DSS05.02	4.2.3.4		A.13.2.1	AC-4, CA-3, CA-9, PL-8
ID	AM	AM-4		APO02.02			A.11.2.6	AC-20, SA-9
ID	AM	AM-5		APO02.02, APO03.04, BAI09.02	4.2.3.6		A.8.2.1	CP-2, RA-2, SA-14
ID	AM	AM-6		APO01.02, DSS06.03	4.3.2.3.3		A.6.1.1	CP-2, PS-7, PM-11

FIGURE 4 NIST CSF complements cybersecurity operations, risk management, and quality management (adapted from Figure 2 in NIST 2014)


Risk Management
Senior Executive Level
Focus: Organizational risk
Actions: Express mission priorities
Approve implementation tier selection
Direct risk decisions
Changes in current and future risk
Mission priority and risk appetite, and budget
ISO 9001
Baldrige
ISO 31000
Business/ Process Level
Focus: Critical infrastructure risk management
Actions: Nominate implementation tiers
Develop profiles
Allocate budget
Framework profiles
NIST CSF
Implementation progress
Changes in assets, vulnerability, and threat
Implementation/ Operations Level
Focus: Securing critical infrastructure
Actions: Implements profile
Cybersecurity Ops
Implementation
©2017, ASQ

conformance is the sum of the cost to prevent issues and the cost to test them (appraisal); the *cost of nonconformance*, also sometimes called cost of rework, is the cost of internal failures added to the cost of external failures; that is, those problems that are recognized, or directly experienced by, customers and other stakeholders. Internal and external failures are distinguished based on *who* is impacted. In many papers, these are referred to as prevention-appraisal-failure (PAF) models. To summarize:

Cost of quality = Cost of conformance
+ Cost of nonconformance

Cost of conformance = Cost of prevention
+ Cost of appraisal

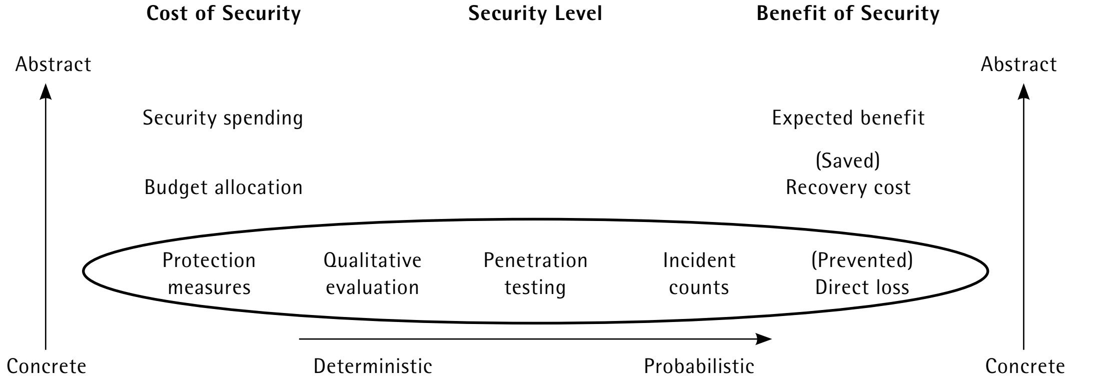
Cost of nonconformance = Cost of internal failures
+ Cost of external failures

Cost of quality = Cost of prevention + Cost of appraisal
+ Cost of internal failures + Cost of external failures

Thomas (2009) proposed a cost of security model based on the loss distribution approach that mentions costs of quality, but does not build on its models. Brecht and Nowey (2013) and Böhme (2010), in their studies of costs in information security, both identified that quality cost models may be appropriate for cybersecurity. Böhme (2010), however, did not mention quality costs directly, but identified the quality cost categories in his articulation of cost/benefit relationships in information security. In Figure 5 on the next page, "protection measures" are prevention, "qualitative evaluation" and "penetration testing" are appraisal, "incident counts" could be categorized by whether the incidents had internal or external impact, and "direct loss" refers to external failures.

Although similar to the production of tangible products in many ways, the development of software is an economically unique activity. Table 1 on the next page identifies some of the differences. Cybersecurity shares many of the same characteristics as software-intensive production; in particular, specifications change extremely rapidly, and defects are related to human understanding of the current state of threats, vulnerabilities, and capabilities. Because of these similarities, and also because so many security controls revolve around software or the software development life cycle (for example, CCS CSC 2) the PAF model for quality costs can be extended to include development activities. In the context of cybersecurity operations, the assumption is made that any of the items that contribute to CoQ also contribute to cost of cybersecurity. As a result, an executive-level dashboard might show two values for

FIGURE 5 Quality costs within cost/benefit relationships in information security (adapted from Böhme 2010)



©2017, ASQ

TABLE 1 Differences between product manufacturing and software-intensive production

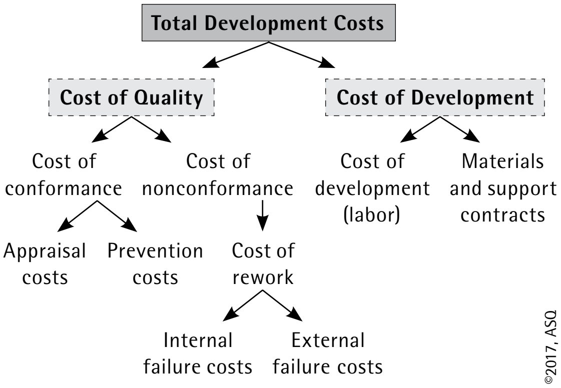
Product Manufacturing	Software-Intensive Production
Physical product	Intellectual product
Output is subject to physical laws and constraints	Output is subject to human constraints and logical constraints
Specification is stable	Specification is constantly changing
Product defects more often the result of faulty materials, machines, or inspection	Product defects more often the result of human mistakes and misunderstandings, or not anticipating ways in which product will be used
Effectively executing processes to satisfy requirements is key	Understanding requirements is key
Marginal cost associated with producing more units of a product	No marginal cost for producing additional product

©2017, ASQ

CoQ: one specific to activities that enhance cybersecurity, and one for other quality-related costs that are not specific to cybersecurity.

Figure 6 shows how costs of quality are related to total development costs. If an organization measures cybersecurity cost of quality (CCoQ) in addition to ordinary CoQ, there will be an additional branch off total development costs. Even though there is only one block in Figure 6 that expressly calls out cost of labor, it is likely that many of the blocks will be dominated by labor costs because of the unique economic aspects of developing the software-intensive systems discussed earlier.

FIGURE 6 Quality costs applied to software development (Radziwill 2006)



©2017, ASQ

Quality Costs in Practice

This model provides great flexibility for organizations that want to examine opportunities for improving resource utilization from several perspectives at once:

Total development costs = Cybersecurity cost of quality + Cost of quality + Cost of development

There are many different ways to use these data. Total development costs, or any of its three components, can be tracked longitudinally on a monthly or quarterly basis. Only cybersecurity CoQ can be tracked, and this can still add value. Total CoQ, ordinary CoQ, and/or cybersecurity CoQ can be expressed as a percentage of total development costs and tracked over time.

For best results, however, data should be collected at the lowest levels of the hierarchy (appraisal, prevention, internal failures, and external failures in CoQ; cost of labor, cost of materials and contracts in cost of

TABLE 2 Examples of cybersecurity activities in quality cost categories.

Quality Cost Category	Cybersecurity Activities (Selected from CIS 2013)
Prevention	CSC 1: Inventory of authorized and unauthorized devices
	CSC 2: Inventory of authorized and unauthorized software
	CSC 3: Secure configurations for hardware and software
	CSC 5: Control use of administrative privileges
	CSC 7: Email and web browser protections
	CSC 8: Malware defenses
	CSC 9: Limit and control ports, protocols, services
	CSC 11: Secure configurations for network devices
	CSC 12: Boundary defense
	CSC 13: Data protection
	CSC 14: Controlled access based on need-to-know
	CSC 15: Wireless access control
	CSC 16: Account control and monitoring
	CSC 18: Application software security
Appraisal	CSC 3: Test secure configurations for hardware and software
	CSC 4: Continuous vulnerability assessment and remediation
	CSC 5: Test use of administrative privileges
	CSC 6: Maintenance and monitoring of audit logs
	CSC 7: Test email and web browser protections
	CSC 8: Test malware defenses
	CSC 9: Test limiting of ports, protocols, services
	CSC 10: Test data recovery
	CSC 11: Test secure configurations for network devices
	CSC 12: Test boundary defense
	CSC 13: Test data protection
	CSC 15: Test wireless access control
	CSC 17: Security skills assessment
	CSC 18: Test application software security
	CSC 20: Penetration tests and red team exercises
Internal Failures	CSC 4: Continuous vulnerability assessment and remediation – respond to internal breaches and notifications from agencies that monitor vulnerabilities
	CSC 5: Respond to internal misuse of administrative privileges
	CSC 10: Respond to internal data recovery issues
	CSC 12: Respond to internal boundary defense issues
	CSC 15: Respond to internal issues that result from wireless access control
	CSC 19: Internal incident response
External Failures	CSC 4: Continuous vulnerability assessment and remediation – respond to external breaches
	CSC 10: Respond to data recovery issues due to external breaches
	CSC 19: External incident response

©2017, ASQ

development). With data organized this way, any of the intermediary categories can also be tracked (for example, cost of nonconformance vs. cost of conformance, or cost of rework). Important patterns that will help managers facilitate improvements to cybersecurity programs can be found in any of these elements, and so some experimentation will be required.

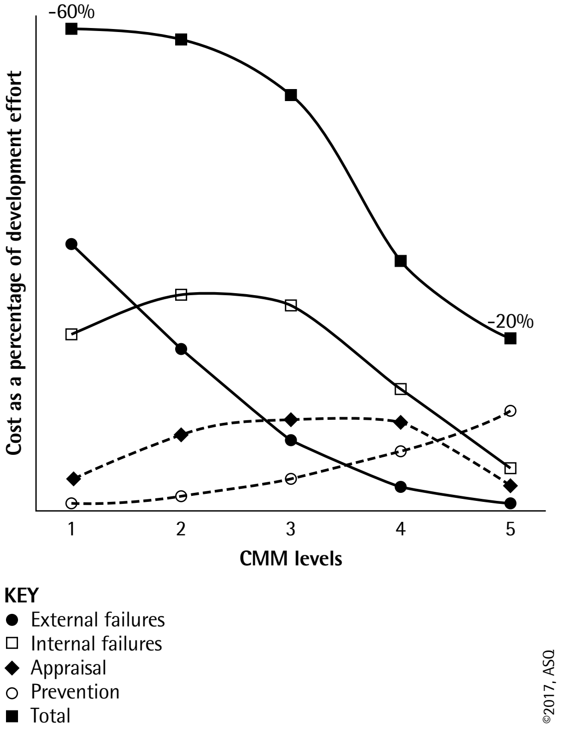
Examples of cybersecurity-related activities that fall into each of the quality cost categories are shown in Table 2. The example activities were drawn from the Center for Internet Security's list of top 20 critical security controls, which provides guidance in the NIST CSF. This list is meant to be illustrative, not exhaustive.

Quality Costs and Organizational Maturity

There has been little work relating the relative levels of quality costs in each category to organizational maturity, and no work to date relating cybersecurity costs of quality to the maturity of an organization's cybersecurity risk management. Several very limited papers exist that show patterns in quality costs for one organization, but these are of limited value because generalizability is low. Of the two models that do exist in the literature (Knox 1993; Sower, Quarles, and Broussard 2007), both indicate nearly the same results: that as an organization matures, total quality costs decrease, but cost of prevention increases to make this possible.

This is illustrated in Figure 7 on the next page from the paper by Knox (1993), who explored quality costs in relation to the maturity of software development processes only. Both appraisal costs and prevention costs follow a similar pattern as well: they peak when an organization has systematic, repeatable processes and

FIGURE 7 Quality costs classified by organizational maturity (CMM 1=low, CMM 5=high). (Knox 1993)



©2017, ASQ

regular, effective training, but then decrease as feedback from learning and integration becomes stronger.

The value of CCoQ will increase as studies are performed to link measured costs from organizations in different industries to maturity levels. Most likely, this maturity would be assessed using tools like the three levels of the C2M2 or the implementation tiers of the Baldrige Cybersecurity Excellence Builder (BCEB), both of which are designed to work well with the NIST CSF. Because the BCEB was not specifically designed to assess maturity, newly proposed structures may be required (Almuhammadi and Alsaleh 2017).

MAPPING OF NIST CSF TO QUALITY COSTS

The primary contribution of this article is a mapping of the 98 subcategories in the NIST CSF to the four main quality cost categories. By categorizing the elements of the NIST CSF at this level, organizations that use the CSF or a similar model can more easily adopt quality costs as a metric.

Methodology

The mapping was produced using a consensus process with two observers (the authors). Independently, each observer classified the 98 NIST CSF subcategories into the four quality cost categories. Multiple classifications were allowed. To distinguish appraisal activities from prevention in the NIST CSF, key words like "audit," "assess," and "verify" were used. To distinguish between appraisal and failures, the likelihood of the appraisal to be ordinary (that is, to *not* detect a failure) was considered. To distinguish between internal failures and external failures, the likelihood of information about a breach reaching a noninsider audience was considered.

Interrater reliability was assessed using Cohen's kappa, with the guideline outlined by Landis and Koch (1977), where the strength of the kappa coefficients = 0.01-0.20 slight; 0.21-0.40 fair; 0.41-0.60 moderate; 0.61-0.80 substantial; 0.81-1.00 almost perfect. Because there were so many subcategories in the NIST CSF that map to both internal and external failures, a fifth category was added for the kappa calculation to reflect this combination. For elements in which one rater marked one quality cost category, and the other rater marked that category plus an additional category, one agreement mark was given for the category in agreement, and one disagreement mark to reflect the disagreement. As a result, 106 ratings were used to compute a kappa of 0.64, indicating substantial agreement. Of the five categories that were assessed for agreement, the strongest agreements were in prevention and the elements that combined internal failures and external failures. The least agreement was for classifications into the internal failures category.

Although a kappa of 0.64 suggests substantial agreement, the next step involved discussing classifications where there was disagreement to determine how a consensus recommendation could be achieved. There were 23 elements that required consensus determination; seven were resolved easily, and 16 required more extensive discussion. The final mapping is shown in the Appendix with annotations. The analysis indicates that greater resolution is needed in the accounting system to accommodate for quality costs associated with several of the NIST CSF subcategories, including:

- **PR.IP-4:** Backups of information are conducted, maintained, and tested periodically: Conducting backups (prevention) should be accounted for separately from testing backup processes (appraisal) to see if they are functioning as anticipated.

- **PR.PT-1:** Audit/Log records are determined, documented, implemented, and reviewed in accordance with policy: Auditing and verification (appraisal) should be tracked separately from developing processes for logs (prevention).
- **RS.RP-1, RS.CO-2 through RS.CO-5, RS.AN-3, RS.AM-4, RS.MI-1, and RS.MI-2:** Need to be accounted for by organizations in more detail, depending upon whether the work was associated with an internal or external failure.
- **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks. This item is complex, encompasses many activities, and may even need to be revisited in the next update of the NIST CSF. When newly identified vulnerabilities are identified, that is an appraisal activity, but when steps are taken to prevent breaches before they occur, that is prevention. Furthermore, the identification of the vulnerability may take place in the context of responding to an internal failure or an external failure.

In addition, care should be taken when charging any activities to the subcategories in the detect (DE) function. Detection occurs prior to the determination of a breach, and does not depend upon the audience that is impacted by that breach. Costs associated with the outcomes of these detections should be accounted for by subcategories in the respond (RS) and recover (RC) functions.

Application

Using the mapping in the Appendix, any work accounting system, such as an organizational work breakdown structure, that is aligned with the NIST CSF can be adjusted to easily report cybersecurity cost of quality. The only change that may be required is to split some elements of the NIST CSF into two so the appropriate quality cost categories can be assessed. Alternatively, if this is not feasible, an organization can create one category called "rework" in which all costs related to recovery from internal and external failures are grouped. Cost of rework may be just as useful a metric, particularly for organizations where a process approach and cybersecurity risk management are not as mature.

The organization can present these data as bar charts or Pareto charts, or it can track the evolution of these values over time on segmented bar charts or in time series. Trends should be examined and discussed by staff and those with decision-making authority to identify opportunities for improvement. All values should be considered with respect to the maturity of the organization, in terms of quality management, risk management, and cybersecurity management. Most importantly, all organizations will require a period of adjustment and calibration when adopting a quality cost approach to help continually improve cybersecurity.

DISCUSSIONS AND CONCLUSIONS

This article presented a mapping of the 98 subcategories in the framework core of the NIST CSF to the four categories of quality costs (prevention, appraisal, internal failure, and external failure). The value of reporting costs of cybersecurity in terms of quality costs lies less in the levels themselves, and more in how the values relate to one another, change over time, and change in response to changes in strategy, organization, or cybersecurity investments. The primary limitation of this study is that the practical applicability of the model can only be assessed through future work on a broad scale: implementation at different organizations, case studies, and empirical research.

Based on this exercise, it became apparent that the NIST CSF does not distinguish between internal and external failures, and this is critical for managing the costs of cybersecurity—unless an organization chooses a simpler quality cost model, and groups internal and external failures to track cost of rework. Furthermore, there are a few subcategories in the NIST CSF that should be segmented in work accounting systems to reflect whether those tasks are being performed as preventive measures, or to test and appraise preventive measures. Organizations may also wish to customize the mapping to better align with their unique systems, structures, and work processes.

Using cybersecurity cost of quality, organizations can answer questions such as:

- Is there enough emphasis on prevention? Typically, unless an organization's process maturity is high, this category will be associated with the greatest costs. If costs of prevention do not occupy the greatest proportion of quality costs, appraisal activities should be reduced in favor of prevention efforts.
- Is there too much or too little time being spent on appraisal (testing)? If too little time is spent on appraisal activities, the cost of rework will be high. An excessively low cost of rework coupled with a high cost of conformance suggests that too much time is being spent on appraisal.
- Is testing aggressive enough that it is triggering internal failures, or is the cost of internal failures small or nonexistent? This is an indication that appraisal efforts should be made more rigorous.

Key questions to be answered in future research include:

- What are the theoretical and empirical relationships between the amount spent on quality cost categories (prevention appraisal, internal failure, external failure) and the amounts spent on each function in the framework core (identify, protect, detect, respond, recover)?
- Does the distribution of cybersecurity costs of quality change in a systematic way as an organization's cybersecurity risk management system matures?
- Does the distribution of cybersecurity costs of quality change in a systematic way as an organization's software life-cycle management matures?
- Do the costs of external failures increase proportionally as the attack surface expands?
- Are the costs of external failures similar for all organizations? Live benchmarking could help organizations identify whether they are being targeted for attacks.

CoQ is a time-tested and well-documented model for identifying and assessing opportunities for improvement that will result in cost savings. By extending this model to cybersecurity risk management using a framework that is well known and widely applied, future empirical research that can provide cost benchmarks and additional methods for anomaly detection is enabled.

REFERENCES

Almuhammadi, S., and M. Alsaleh. 2017. Information security maturity model for NIST cybersecurity framework. *Computer Science & Information Technology* 51.

Böhme, R. 2010. Security metrics and security investment models. *IWSEC* (November):10-24.

Brecht, M., and T. Nowey. 2013. A closer look at information security costs. *The Economics of Information Security and Privacy.* Berlin, Germany: Springer Berlin Heidelberg.

Campanella, J. 1999a. Principles of quality costs: Principles, implementation, and use. In *ASQ World Conference on Quality and Improvement Proceedings*, 507. Milwaukee, WI: American Society for Quality.

Campanella, J. 1999b. *Quality costs: Principles and implementation and use*, third edition. Milwaukee, WI: ASQ Quality Press.

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou. 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security* 11, no. 3:431-448.

CIS. 2013. Center for cybersecurity top 20 critical security controls (CCS CSC). New York, NY: Center for Internet Security (CIS). Available at: https://www.cisecurity.org/controls/.

Clauson, J. 1995. Cyberquality: Quality resources on the internet. *Quality Progress* 28, no. 1:45.

Farwell, J. P., and R. Rohozinski. 2011. Stuxnet and the future of cyber war. *Survival* 53, no. 1: 23-40.

Gordon, L. A., M. P. Loeb, and L. Zhou. 2011. The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security* 19, no. 1:33-56.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou. 2015. Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security* 6:24-30. Available at: http://dx.doi.org/10.4236/jis.2015.61003.

ISACA. 2012. COBIT 5 – Control Objectives for Information and Related Technologies. (ISACA Standard no. COBIT 5). Rolling Meadows, IL: Information Systems Audit and Control Association (ISACA). Available at: http://www.isaca.org/COBIT/Pages/default.aspx.

ISA/IEC. 2013. Security for industrial automation and control systems. (ISA Standard no. 62443). Research Triangle Park, NC: International Society of Automation (ISA). Available at: https://www.isa.org/isa99/.

ISO/IEC. 2016. Information security management. (ISO/IEC standard no. 27001). Geneva, Switzerland: International Organization for Standardization. Available at: https://www.iso.org/isoiec-27001-information-security.html.

Knox, S. T. 1993. Modeling the cost of software quality. *Digital Technical Journal* 5, no. 9-9.

Landis, J. R., and G. G. Koch. 1977. The measurement of observer agreement for categorical data. *Biometrics* 33, 159-174.

Miron, W., and K. Muita. 2014. Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review* 4, no. 10.

Moore, T., S. Dynes, and F. R. Chang. 2016. Identifying how firms manage cybersecurity investment. Berkeley, CA: University of California, Berkeley.

NIST. 2013. NIST Special Publication 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. Washington, DC: National Institute of Standards and Technology.

NIST. 2014a. Framework for improving critical infrastructure cybersecurity, version 1.0. Washington, DC: National Institute of Standards and Technology. Available at: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=915385.

NIST. 2014b. Framework core. Washington, DC: National Institute of Standards and Technology. Available at: https://www2.nist.gov/file/270221.

NIST. 2014c. Alternative view of framework core. Washington, DC: National Institute of Standards and Technology. Available at: https://www2.nist.gov/file/270226.

Obama, B. 2013. Feb 12. Executive order #13636: Improving critical infrastructure cybersecurity. *Federal Register* 78, no. 33:11739.

Radziwill, N. M. 2006. Cost of quality (CoQ) metrics for telescope operations and project management. In *Proceedings of SPIE* (vol. 6271, 627104-1). Available at: http://dx.doi.org/10.1117/12.669399.

Radziwill, N. M., and M. C. Benton. 2017. Design for X (DfX) in the Internet of Things (IoT). *Journal of Quality Management Systems, Applied Engineering, & Technology Management (JoQAT)* 1.

S. 1353. 2014. 113th Congress. Cybersecurity Enhancement Act of 2014 (enacted). Available at: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

SANS. 2016. Critical security controls, version 6.0. Bethesda, MD: SANS. Available at: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf.

Schiffauerova, A., and V. Thomson. 2006. Managing cost of quality: Insight into industry practice. *The TQM Magazine* 18, no. 5:542-550.

Sower, V. E., R. Quarles, and E. Broussard. 2007. Cost of quality usage and its relationship to quality system maturity. *International Journal of Quality & Reliability Management* 24, no. 2:121-140.

Thomas, R. C. 2009. Total cost of security: A method for managing risks and incentives across the extended enterprise. In *Proceedings of the 5th Annual Workshop on Cyber Security and information intelligence Research: Cyber Security and information intelligence Challenges and Strategies.* ACM.

Trautman, L. J., and P. C. Ormerod. 2017. Industrial cyber vulnerabilities: Lessons from Stuxnet and the Internet of Things. Available at SSRN: https://ssrn.com/abstract=2982629.

BIOGRAPHIES

Nicole Radziwill is an associate professor in the Department of Integrated Science and Technology (ISAT) at James Madison University (JMU) in Harrisonburg, VA. She is a Fellow of ASQ and is a Certified Six Sigma Black Belt (CSSBB) and Certified Manager of Quality/Organizational Excellence (CMQ/OE). She has a doctorate in quality systems from Indiana State University, and her research focuses on the quality and innovation in cyber-human production systems. She is one of ASQ's Influential Voices and blogs at http://qualityandinnovation.com.

Morgan Benton is co-founder of the Burning Mind Project, and an associate professor in the Department of Integrated Science and Technology (ISAT) at James Madison University (JMU) in Harrisonburg, VA. He holds a doctorate and a master's degree in information systems from the New Jersey Institute of Technology, and a bachelor's degree in leadership studies/sociology/physics from the University of Richmond. His research focuses on innovation in learning, higher education, and transformation.

APPENDIX: Mapping of the NIST CSF to the four quality cost categories

			QUALITY COST CATEGORY			
Function	**Category**	**Subcategory**	**Prevention**	**Appraisal**	**Internal Failure**	**External Failure**
Identify (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	X			
		ID.AM-2: Software platforms and applications within the organization are inventoried	X			
		ID.AM-3: Organizational communication and data flows are mapped	X			
		ID.AM-4: External information systems are catalogued	X			
		ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	X			
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	X			
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated	X			
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	X			
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	X			
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	X			
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)	X			
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	X			
		ID.GV-2: Information security roles and responsibilities are coordinated and aligned with internal roles and external partners	X			
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	X			
		ID.GV-4: Governance and risk management processes address cybersecurity risks	X			

APPENDIX: Mapping of the NIST CSF to the four quality cost categories *(Continued)*

			QUALITY COST CATEGORY			
Function	Category	Subcategory	Prevention	Appraisal	Internal Failure	External Failure
Identify (ID) **Cont'd**	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	X			
		ID.RA-2: Cyber threat intelligence and vulnerability information is received from information sharing forums and sources	X			
		ID.RA-3: Threats, both internal and external, are identified and documented	X			
		ID.RA-4: Potential business impacts and likelihoods are identified	X			
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	X			
		ID.RA-6: Risk responses are identified and prioritized	X			
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	X			
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	X			
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis	X			
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess, and manage supply chain risks.	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	X			
		ID.SC-2: Identify, prioritize, and assess suppliers and partners of critical information systems, components, and services using a cyber supply chain risk assessment process	X			
		ID.SC-3: Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the information security program or cyber supply chain risk management plan	X			
		ID.SC-4: Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted		X		
		ID.SC-5: Response and recovery planning and testing are conducted with critical suppliers/providers		X		

©2017, ASQ

APPENDIX: Mapping of the NIST CSF to the four quality cost categories *(Continued)*

			QUALITY COST CATEGORY			
Function	**Category**	**Subcategory**	**Prevention**	**Appraisal**	**Internal Failure**	**External Failure**
Protect (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	X	X		
		PR.AC-2: Physical access to assets is managed and protected		X		
		PR.AC-3: Remote access is managed		X		
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties		X		
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate		X		
		PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate		X		
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	X			
		PR.AT-2: Privileged users understand roles and responsibilities	X			
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	X			
		PR.AT-4: Senior executives understand roles and responsibilities	X			
		PR.AT-5: Physical and information security personnel understand roles and responsibilities	X			
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	X			
		PR.DS-2: Data-in-transit is protected	X			
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	X			
		PR.DS-4: Adequate capacity to ensure availability is maintained	X			
		PR.DS-5: Protections against data leaks are implemented	X			
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity		X		
		PR.DS-7: The development and testing environment(s) are separate from the production environment	X			
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity		X		

APPENDIX: Mapping of the NIST CSF to the four quality cost categories *(Continued)*

			QUALITY COST CATEGORY			
Function	**Category**	**Subcategory**	**Prevention**	**Appraisal**	**Internal Failure**	**External Failure**
Protect (PR) **Cont'd**	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g., concept of least functionality)	X			
		PR.IP-2: A system development life cycle to manage systems is implemented	X	X		
		PR.IP-3: Configuration change control processes are in place	X			
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically		X		
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	X	X		
		PR.IP-6: Data is destroyed according to policy	X			
		PR.IP-7: Protection processes are continuously improved		X		
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	X			
		PR.IP-9: Response plans (incident response and business continuity) and recovery plans (incident recovery and disaster recovery) are in place and managed	X			
		PR.IP-10: Response and recovery plans are tested		X		
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	X			
		PR.IP-12: A vulnerability management plan is developed and implemented	X			
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	X			
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	X			

APPENDIX: Mapping of the NIST CSF to the four quality cost categories *(Continued)*

			QUALITY COST CATEGORY			
Function	Category	Subcategory	Prevention	Appraisal	Internal Failure	External Failure
Protect (PR) **Cont'd**	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/Log records are determined, documented, implemented, and reviewed in accordance with policy	X	X		
		PR.PT-2: Removable media is protected and its use restricted according to policy	X			
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	X			
		PR.PT-4: Communications and control networks are protected	X			
		PR.PT-5: Systems operate in pre-defined functional states to achieve availability (e.g., under duress, under attack, during recovery, normal operations)	X			
Detect (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	X			
		DE.AE-2: Detected events are analyzed to understand attack targets and methods		X		
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors		X		
		DE.AE-4: Impact of events is determined		X		
		DE.AE-5: Incident alert thresholds are established	X			
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events		X		
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events		X		
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events		X		
		DE.CM-4: Malicious code is detected		X		
		DE.CM-5: Unauthorized mobile code is detected		X		
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events		X		
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed		X		
		DE.CM-8: Vulnerability scans are performed		X		

APPENDIX: Mapping of the NIST CSF to the four quality cost categories *(Continued)*

			QUALITY COST CATEGORY			
Function	Category	Subcategory	Prevention	Appraisal	Internal Failure	External Failure
Detect (DE) **(Cont'd)**	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	X			
		DE.DP-2: Detection activities comply with all applicable requirements	X			
		DE.DP-3: Detection processes are tested		X		
		DE.DP-4: Event detection information is communicated to appropriate parties	X	X		
		DE.DP-5: Detection processes are continuously improved	X	X		
Respond (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event			X	X
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-1: Personnel know their roles and order of operations when a response is needed	X			
		RS.CO-2: Events are reported consistent with established criteria			X	X
		RS.CO-3: Information is shared consistent with response plans			X	X
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans			X	X
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness				X
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated		X		
		RS.AN-2: The impact of the incident is understood		X		
		RS.AN-3: Forensics are performed			X	X
		RS.AN-4: Incidents are categorized consistent with response plans			X	X
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained			X	X
		RS.MI-2: Incidents are mitigated			X	X
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks			X	X

APPENDIX: Mapping of the NIST CSF to the four quality cost categories *(Continued)*

			QUALITY COST CATEGORY			
Function	**Category**	**Subcategory**	**Prevention**	**Appraisal**	**Internal Failure**	**External Failure**
Respond (RS) **(Cont'd)**	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/ response activities.	RS.IM-1: Response plans incorporate lessons learned	X			
		RS.IM-2: Response strategies are updated	X			
Recover (RP)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event			X	X
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	X			
		RC.IM-2: Recovery strategies are updated	X			
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, internet service providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed				X
		RC.CO-2: Reputation after an event is repaired				X
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams			X	X