

Is Information Security Under Control?

Investigating Quality in Information Security Management

Previous studies of organizations' use of information security controls have focused on the presence or absence of controls, rather than their quality. According to the authors' survey focusing on control quality, implementation quality varies significantly by organization size as well as industry.



WADE H.
BAKER AND
LINDA
WALLACE
Virginia Tech

Over the past decade, organizations have sought to become more efficient and productive by adopting information and communication technologies. As such ICTs become more common, their intrinsic value is dwarfed by the mission-critical functions they support.¹ This intimate relationship between technology and business functionality has proven to be an incubator for a dramatic increase in costly information security incidents and failures leading to substantial revenue losses. Organizations are consequently more aware of information security risks and the need to take appropriate action. However, with so many security options available, many organizations struggle to identify the best ways to counteract the threats they face.

Seeking to protect the confidentiality, integrity, and availability of ICT-supported business functions, the information security industry now boasts a diverse set of products, services, processes, and policies ranging from complex mathematical encryption algorithms to human resource management and federal legislation. Leveraging this array of controls, many organizations have begun formal information security management programs in an effort to protect themselves and their partners and customers. The high implementation and maintenance costs of security controls are increasing pressure on managers to distinguish between controls their organizations need and those that are less critical. Moreover, identifying the optimal level at which to implement individual controls is a delicate balance of risk reduction and cost efficiency.

Unfortunately, for many of these programs, managing security risk has become more about quantity than quality. Because they're unsure of the best controls for their situations, managers often deploy as many as possible,

without regard to their quality or effectiveness. In some instances, controls intended to correct security deficiencies actually add deficiencies to the system.² Information security management should take a lesson from the long-established quality management paradigm: incidents indicate defects in the organization's security program. Organizations must therefore increase quality by rationally implementing the controls necessary to minimize defects and ensure continued business functionality. Amid numerous vulnerabilities, complex threats, greater regulation, and shrinking budgets, the payoff for meeting the challenge is clear: when organizations can identify the appropriate controls for their situations and implement them efficiently, they can effectively manage information security risks.³

We designed and conducted a survey as an initial step toward meeting this challenge. To do this, we benchmarked how organizations manage information security by implementing various controls. Although security surveys are nothing new, our method aims to uncover specific details of control implementation and focus on implementation quality. With a more precise understanding of current practices, information security management can begin to properly pursue effective strategies to improve quality and lower risk.

Information security controls

Many early information security programs relied heavily on technological innovations. Organizations deployed new security products to lock down networked resources, thereby establishing a safe perimeter in which to conduct business. This approach was reasonable because

many of the assets requiring protection were also highly technical. When used correctly, these techniques significantly reduce security incidents within the enterprise. However, as successful and sophisticated as these technologies have become, technical approaches alone can't solve security problems for the simple reason that information security isn't merely a technical problem. It's also a social and organizational problem.⁴ As it has matured, the information security discipline has progressed to recognize the importance of a holistic approach to securing technology, processes, people, and other organizational factors on an enterprise scale.

The US National Institute of Standards and Technology classifies information security controls into three categories⁵:

- *Technical* controls traditionally include products and processes (such as firewalls, antivirus software, intrusion detection, and encryption techniques) that focus mainly on protecting an organization's ICTs and the information flowing across and stored in them.
- *Operational* controls include enforcement mechanisms and methods of correcting operational deficiencies that various threats could exploit; physical access controls, backup capabilities, and protection from environmental hazards are examples of operational controls.
- *Management* controls, such as usage policies, employee training, and business continuity planning, target information security's nontechnical areas.

In this study, we designate controls to one of these three categories. This distinction is important because the type and quality of an organization's controls indicate the maturity of its overall security management program. Using this categorization scheme, we can also determine whether organizations are focusing on technical and operational controls to the detriment of management controls or vice versa. Given security controls' technical origins, we suspect that many security programs still focus on technical and operational practices and overlook management controls, such as policy development.

As Microsoft vice president Dave Thompson has said, "Security is a journey, not a destination."² With the evolving nature of security controls, consistent research aimed at discovering where organizations are along this journey should be beneficial. As a result, several studies in the past 10 years have focused on various organizations' adoption of security controls. The Computer Security Institute and US Federal Bureau of Investigation, for example, regularly administer the Computer Crime and Security Survey⁶ to identify and establish trends. Although the CSI/FBI survey and other similar studies reveal important changes in organizational security practices over time, several key issues have limited their potential value.

First, although surveys commonly ask about the use of

various controls, such as antivirus software and backup procedures, the questions aren't at a level of detail that could reveal critical limitations in the controls' effectiveness. For instance, knowing that an organization uses antivirus software is much less important than uncovering specific details about which systems have antivirus software installed, whether the antivirus software provides full-time protection, or how often the organization updates virus definitions.⁷

Second, because survey questions have typically been binary (yes or no) in nature, control implementation quality remains mostly unknown. In fact, we're unaware of any surveys in the security domain that target control quality. Most security professionals would agree that a firewall doesn't achieve full effectiveness simply by being plugged into the network. Once installed, simple variations in rule sets, location, and administration contribute to the device's quality. You might answer "yes" to a question asking if you use antivirus software, when in reality the software might be poorly configured, inadequately maintained, and installed on only a few systems. A study focusing on a control implementation's comprehensiveness could give a clearer picture of the information security management's state than a study asking simply whether a control is used.

Finally, because of security and privacy concerns, organizations are often (rightly) reluctant to divulge specific or complete descriptions of their security practices, making the collection of quality information a difficult process, especially for academia and smaller private entities.⁸

Survey methodology

To better understand how organizations use controls to manage information security risk, we created a Web-based survey addressing 80 specific security practices in 16 general security domains (see Table 1). A group of 10 security experts from industry and academia helped us identify the 80 controls in our survey. These controls constitute a well-balanced information security management program and represent a cross-section of controls found in several international standards, including British Standard 7799, NIST Special Publication 800-53, the

Technical approaches alone can't solve security problems for the simple reason that information security isn't merely a technical problem.

Graham-Leach-Bliley Act of 1999, and the North American Electric Reliability Council's Urgent Action Standard 1200.

We solicited survey participants from a listserv of se-

Table 1. Major security domains and number of controls they address.

GENERAL SECURITY CONTROL DOMAINS	NUMBER OF CONTROLS
Antivirus software	4
Backup and recovery	5
Business continuity/incident response	5
Employee training and awareness	6
Help desk/IT support training	4
Staff hiring and termination	4
Monitoring and logging	4
Network auditing and logging	6
Network security management	6
Passwords and access control	4
Physical security	9
Remote access security	4
Sensitive data handling and protection	6
System-level security	4
Technical documentation	4
Testing and review	5
Total	80

curity practitioners. Our email invitation described the study and offered access to the results as an incentive for participation. We sent subsequent follow-ups and reminders during the two weeks the survey was active.

Respondents included information security executives, managers, and technical specialists. The 349 respondents were North America (71 percent), Europe (18 percent), Asia-Pacific (10 percent), and South America (1 percent). Of the represented organizations, 34 percent had fewer than 100 computer systems, 38 percent had between 101 and 1,000, and 28 percent had more than 1,000 systems. Respondents selected from a list of 30 industries, which we grouped into services (27 percent), information technology (20 percent), government (14 percent), production (14 percent), education (11 percent), and finance (13 percent) for analysis purposes.

We made the survey anonymous to gain participants' trust and made it clear that there would be no way to track responses to an individual respondent or to their organization. To further provide credibility and encourage participation,⁸ we conducted the study in cooperation with Cybertrust, a global security services company.

We asked participants to rate the quality of their organizations' current implementations for each of the 80 practices, according to the scale in Table 2. They could choose "unsure" if they were unfamiliar with their organizations' adherence to a particular control.

Analysis results

Figure 1 summarizes responses to our survey concerning two practices involving antivirus software. The 2004

CSI/FBI survey, by contrast, is substantially less descriptive, reporting only that antivirus software usage was 99 percent.⁶ Our results indicate that the CSI/FBI number might be a little misleading because several important issues surround the use of antivirus controls (for example, the percentage of desktops covered and whether the organization has a policy mandating antivirus software use), and organizations don't always implement controls at the highest quality level. For example, only 67 percent of the respondents to our survey said that their organization comprehensively implemented antivirus software and about 30 percent of them rated their antivirus policy as below average or worse.

Controls with highest and lowest implementation quality

Our first goal was to identify the controls that organizations, on average, implement comprehensively (a 6 rating) versus controls that they implement poorly (a 1 rating). Figure 2 (p. 40) shows the 10 controls that respondents rated the highest in terms of implementation quality. Not surprisingly, antivirus practices occupy the top three spots and are the only controls with an average quality rating of 5 (advanced) or above. Viruses and malicious code represent some of the more obvious and persistent security risks, so most organizations are diligent in mitigating the threats they pose. Respondents gave two other well-known controls—backups and system patching—the next highest scores, although quality varied more than with antivirus controls, as the stacked bar graphs in Figure 2 show.

Our results also show that organizations are focusing on technical documentation, at least in the areas of network characteristics and critical device administration. Outside the top 10, the picture of implementation quality is somewhat less optimistic. Respondents rated only one additional control above 4 (above average)—a fact we found both surprising and disturbing.

Of the 80 controls included in the study, respondents rated those listed in Figure 3 (p. 41) as being the lowest quality. In light of the rapid growth of the mobile workforce and remote connections, we didn't expect the identification and tracking of modem connections to receive the lowest rating. These connections often provide direct access to critical systems and are a significant source of risk that shouldn't be neglected.

Another poorly implemented control involves training personnel to prevent social engineering attacks. All employees, especially those with access to or knowledge of systems containing sensitive information, are choice targets of social engineering tactics, and it appears that organizations might not be adequately preparing their employees to counter these threats. Organizations must also be able to detect incidents and remedy their impact.⁴ Still, business continuity/incident response controls ap-

Table 2. Scale for rating implementation quality.

NUMERICAL SCORE	DEFINITION	DESCRIPTION
0	Not implemented	The organization doesn't implement the practice at all.
1	Poor	Although the practice might provide some benefit for the organization, it is incomplete, low quality, and not rationalized.
2	Below average	The implementation doesn't meet all requirements or doesn't meet them well.
3	Average	The implementation might be a "work in progress" or simply of mediocre quality.
4	Above average	The organization has implemented the control fairly well, with possibly some enforcement and documentation.
5	Advanced	The control is mostly to fully implemented, with at least some enforcement and documentation.
6	Comprehensive	The control is fully implemented, well thought-out, strictly enforced, and thoroughly documented.

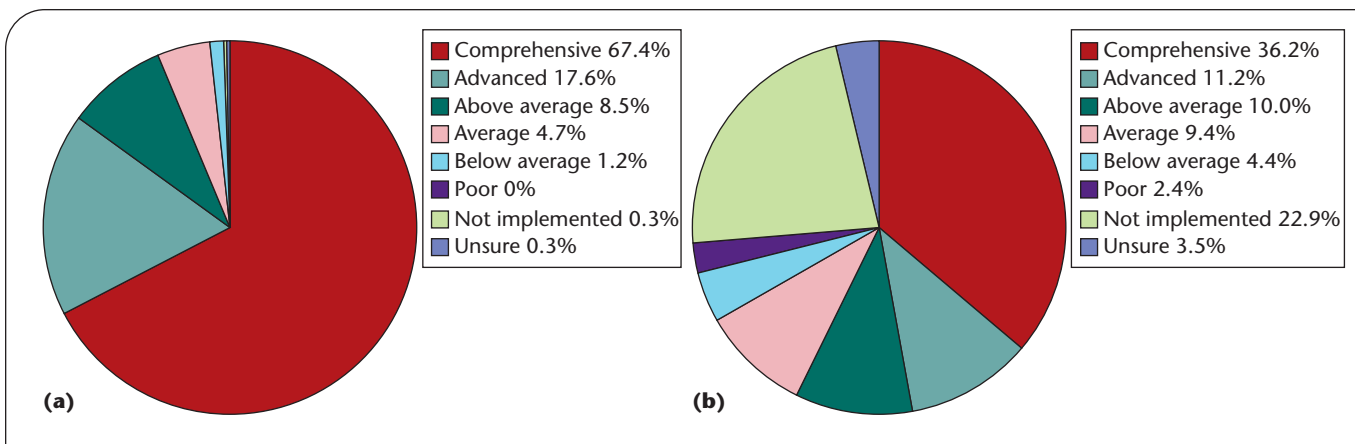


Figure 1. Breakdown of quality ratings for two questions relating to antivirus controls. In survey respondents' organizations, antivirus software is (a) deployed on at least 90 percent of all desktop PCs, and (b) mandated by a formal written policy.

pear frequently in Figure 3, with three of the five control practices in this domain included in the bottom 10.

It's also surprising that respondents rated real-time alerting in the event of a security breach as inferior because organizations surveyed in other security studies have reported high usage of intrusion-detection systems. Organizations that have detection systems without real-time alerts are like houses filled with smoke detectors that have no alarm mechanisms. This once again demonstrates that some security studies might not be asking questions at a level detailed enough to detect subtle differences that could prove critical to the security programs' success.

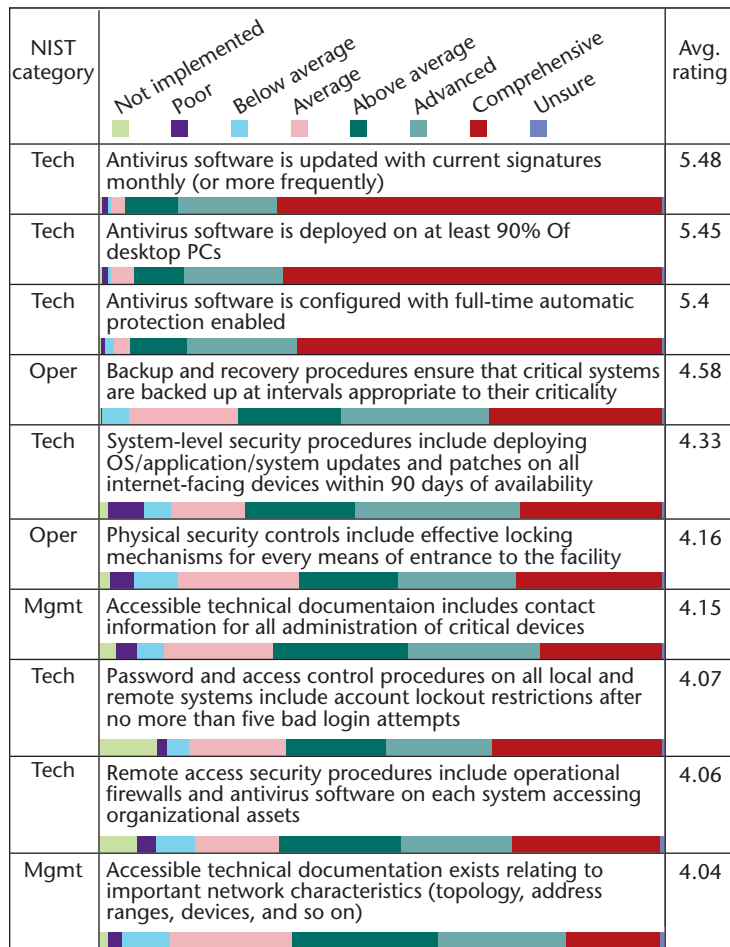
**Management controls:
The role of policy in quality**

An analysis of the NIST control categories represented in Figures 2 and 3 reveals an important trend: only two of the top 10 are management controls (and even these have a strong technical focus), whereas six management controls appear in the bottom 10. Extending this line of analysis beyond the controls listed in Figures 2 and 3, we found that of all 80 practices surveyed, management con-

trols had substantially lower implementation ratings than controls in the technical and operational categories. These findings aren't without real-world relevance because many management controls help define "security" in the context of the organization's mission and clarify the activities and procedures that are and aren't allowed.⁹ Organizations must realize that a large proportion of information security problems extend far beyond technology⁴ and learn to appreciate the role that less technical controls, such as policy development, play in minimizing security breaches' impact on mission-critical operations.

Differences in perceptions of the value of policies and other management controls might explain some of the substantial disparity in control quality among organizations in our study. To empirically assess the value added by management controls, we tested the statistical relationship between security policies and the implementation level of related controls in the four security domains containing a policy-related question. (That we examine policies for only four of the 16 security domains isn't an attempt to claim that other areas don't need policy.) To accomplish this, we compared organizations rating their

Information Security Controls



*Note: The first few words of each control relate it to one of the 16 major security domains shown in Table 1

Tech = Technical Oper = Operational Mgmt = Management

Figure 2. Controls with the highest implementation quality rating.

security policies' quality as below average with those rating their policies as above average. Table 3 lists the results of the analysis of variance (ANOVA) tests for differences between the two groups.

As evident in Table 3 (p. 42), organizations that rated the governing policy implementation as above average gave a significantly higher quality rating for all nonpolicy controls. This correlation suggests that strong policies improve quality and that management controls play a vital role in an organization's commitment to security. Furthermore, it demonstrates how 1D approaches can be detrimental and helps strengthen the argument for a holistic approach to security. Our survey doesn't aim to prove causality between security policies and improved control quality, so other factors that we didn't uncover could be responsible for the correlation. Policies have no innate capabilities for improving the implementation of technical

controls, and it's likely that the effects observed in Table 3 are partially a result of organizations having mechanisms in place to enforce these policies. In any event, the results in Table 3 are compelling enough to warrant future research.

Variation by size

Many surveys have shown that organizational size affects the adoption of certain security controls. These findings seem reasonable, given that larger organizations likely have larger budgets for information-security-related expenses. On the other hand, implementation difficulty would likely increase as well, potentially lowering control quality. Therefore, we examined how implementation quality differed by organization size. We divided respondents into three categories based on the number of computers within the organization. Small organizations had 100 or fewer computers, medium organizations had 100–1,000 computers, and large organizations had more than 1,000 computers.

In almost every case, our results showed that controls have a higher implementation quality within larger organizations. However, the difference was statistically significant for only about 25 percent of the controls. Figure 4 (p. 43) shows the security practices that varied the most by organization size. These differences were predominately limited to two major domains: network security management and physical security. Given that a network's complexity and the physical location's square footage are likely to increase with an organization's size, we'd expect large firms to exert more diligence in protecting these assets.

However, smaller organizations can't afford lax security just because they have fewer resources. These organizations should assess whether their decreased attention to these areas increases their exposure to related threats. Another interesting finding is that of all 80 controls we surveyed, only one—reviewing network logs on a weekly basis—had a higher implementation rating as organization size decreased. We interpret this result to reflect the sheer difficulty of comprehensively and consistently auditing logs generated by increased traffic on larger networks.

Variation by industry

In addition to organization size, we expected control quality to vary among the industries participating in our survey. At first glance, our results show that the variation in implementation quality across industries is highly significant for many controls. Further review reveals that just two of the industry groups are responsible for the disparity—education and finance. Although the average control ratings vary slightly among the service, production, government, and IT industry groups, none of the differences were statistically significant.

Without exception, the education industry reported lower scores than all other groups for each of the 80 controls surveyed, whereas finance typically scored the highest. Figure 5 (p. 44) clearly demonstrates this trend by

plotting the implementation quality rating in the 16 major security domains for the six industry groups. As you can see, respondents in the education industry rated 12 of the 16 security domains below 3 (average). In light of numerous major information security incidents reported within educational institutions in recent years, these results are extremely telling.

Although the free exchange of information and decentralization are staples of higher education, these organizations need comprehensive security programs to protect both the institutions and the individuals within them. Individuals outside of academia can also be affected, as institutions of higher education are notorious staging grounds for malicious activity directed toward government or commercial organizations. Limited budgets, inadequate security staffs (often consisting of a few part-time graduate students), and departmental autonomy make security efforts more difficult. Conversely, financial institutions often have larger and highly trained security departments backed by ample budgets. Increased pressure from customers, partners, and regulatory agencies to secure their assets and processes can provide additional impetus toward higher levels of control implementation.

The disparity exhibited in Figure 5 could also stem from the fact that each industry operates in a somewhat unique risk environment. Research has shown that attack rates, vulnerabilities, and impact from security incidents vary among industries.^{10,11} We can therefore conclude that security efforts are somewhat related to these factors and that organizations operating in riskier environments exert more diligence in protecting themselves.

Control quality's effect on reported incidents

A rather crucial line of analysis at this point involves whether any empirical evidence shows that quality matters in an information security program. To test the relationship between control quality and security incidents, we asked participants if any of 10 common types of information security incidents had impacted their organizations in the year before the survey. Table 4 (p. 43) shows the results, comparing these responses to their overall security programs' implementation quality (the mean score of all 80 controls).

As the table shows, organizations with poor implementation quality (a mean score of 0–2) were more likely to report incidents than those with advanced security programs (a mean score of 5–6). Although organizations reporting superior implementation scores might simply underreport incidents (or vice versa), these results suggest that higher quality controls lower the probability of security incidents. The improvement is substantial for some incident types (such as data theft via network breach) yet less so for others (such as errors and omissions), hinting that the benefits of higher quality vary among control and threat combinations. Although not apparent in Table 4,

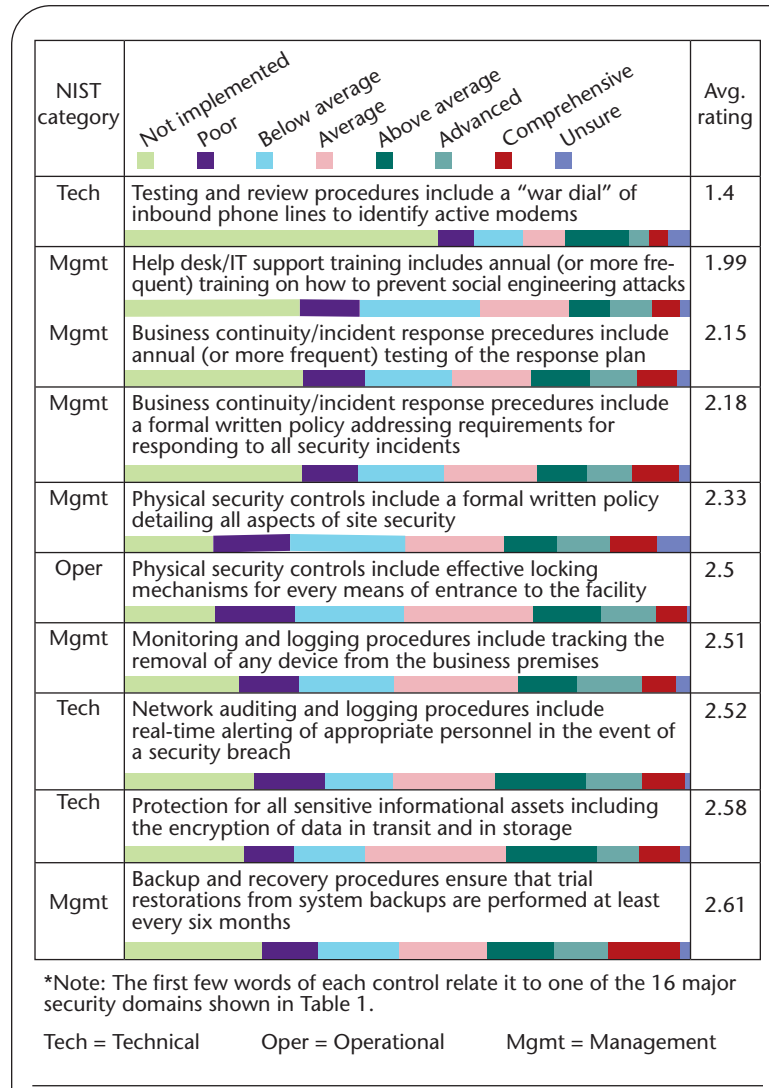


Figure 3. Controls with the lowest implementation quality rating.

our data show that organizations reporting high-level technical controls but low-level management and operational controls were more likely to report incidents than those with high scores across all three types of controls. This seems to support the notion that an unbalanced security program is less effective than a more balanced one, and further supports holistic security measures.

As Figure 6 (p. 44) demonstrates, certain types of threats respond differently as a security program's quality improves. As implementation quality increases from poor to advanced, the percentage of organizations reporting virus and malicious code incidents drops sharply at first and then levels out. Assuming that cost increases with control implementation, it wouldn't appear beneficial for an organization desiring to reduce virus infections to achieve maximum quality. Alternatively, insider network intrusions exhibit a somewhat different behavior: the incident rate declines initially but shows almost no further reduction until imple-

Table 3. The effect of policy on control quality ratings.

POLICY QUALITY	AVERAGE CONTROL RATING	
	BELOW AVERAGE	ABOVE AVERAGE
<i>Antivirus software</i>		
90-percent deployment	6.07	6.64
Updated monthly	6.09	6.71
Full-time protection	5.97	6.64
<i>Business continuity/incident response</i>		
Assessing device criticality	3.44	5.87
Delineation of responsibility	2.84	5.81
Training for response team members	2.53	5.35
Testing of response plan	2.05	5.29
<i>Physical security</i>		
Locking mechanisms on entrances	4.44	6.32
Access control to critical areas	3.14	5.75
Monitoring activities in facility	2.82	5.70
Restriction of ingress via infrastructure	2.76	5.69
Protection from environmental hazards	3.19	5.76
Preventing access to infrastructure	3.07	5.61
Equipment locked in racks and cabinets	2.92	5.58
Alerts in the event of physical breach or failure	2.72	5.49
<i>Sensitive data handling and protection</i>		
Training on the use and handling of sensitive data	2.49	5.36
Labeling of all system outputs	2.70	4.80
Disposal of sensitive information	2.96	5.48
Review of applicable laws and regulations	2.65	5.37
Encryption of data in transit and storage	2.39	5.05

Note: The p-values for all ANOVA tests were highly significant with levels less than .0001.

mentation quality reaches advanced levels. In this case, the organization might find the additional effort and expenditure required to maximize quality worthwhile.

Larry Gordon and Marty Loeb¹² point out that fully implementing every available control isn't an efficient use of resources and that organizations should invest in security only to the point at which marginal benefit equals marginal cost. Although they apply this principle to organizations as a whole, it logically applies to individual controls as well. It might be possible, for instance, to optimize return on investment by implementing three controls at an average level rather than a single control at a comprehensive level. Researchers in the quality management field have used Armand Feigenbaum's four costs of quality¹³ to derive optimum quality levels in systems. Feigenbaum's work also potentially offers valuable insight for efficiently managing information security

Today's organizations appear to be actively seeking to control information security, but they're going about this process in significantly different ways. Overall, many organizations are managing security in a somewhat in-

consistent and superficial manner. Rather than taking a calculated or rational approach, they're emphasizing certain controls while leaving others, though no less important, poorly maintained.

We suspect that the superior control quality reported by the finance industry is at least somewhat related to strict regulations and well-supplied security departments. In light of recent trends toward increased legislation and compliance requirements, examining the effect of regulations on security-program quality and success is an intriguing area for future research.

Although this study gives a more accurate account of the current state of information security management than many previous studies, it can't tell whether the unimpressive quality levels result from organizations' predetermined efforts to optimally implement each control. However, most organizations are unlikely to attempt to conduct such calculations. As a step toward remedying this situation, researchers and professionals should move away from simplistic binary investigation and security practice trending to a more analog view of controls. Organizations can use our survey to gain insight into their security programs' quality and efficacy with little addi-

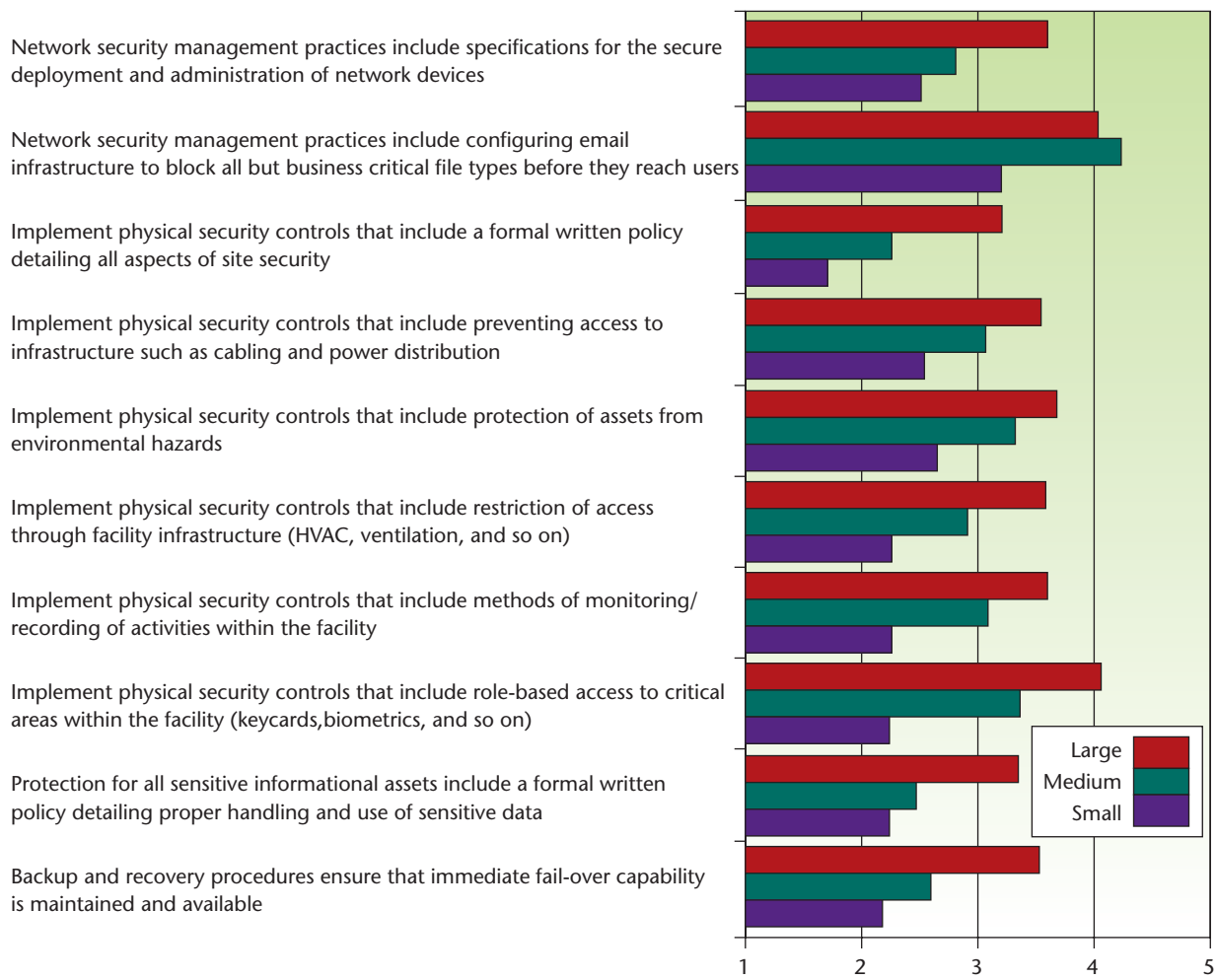


Figure 4. Controls exhibiting significant quality differences by organization size.

Table 4. Effect of program quality on reported security incidents.

TYPE OF INCIDENT REPORTED	REPORTING INCIDENTS (%)	
	LOW-SCORING PROGRAMS (0–2)	HIGH-SCORING PROGRAMS (5–6)
Viruses and malicious code	85	42
Network intrusion by outsiders	67	30
Network denial-of-service attacks	31	16
Data theft via network breach	62	18
Internet and electronic fraud	54	33
Network intrusion by insiders	67	33
Misuse or abuse of resources by insiders	85	61
Errors and omissions	92	85
Data theft via breach of premises	31	13
Physical denial of service	38	27

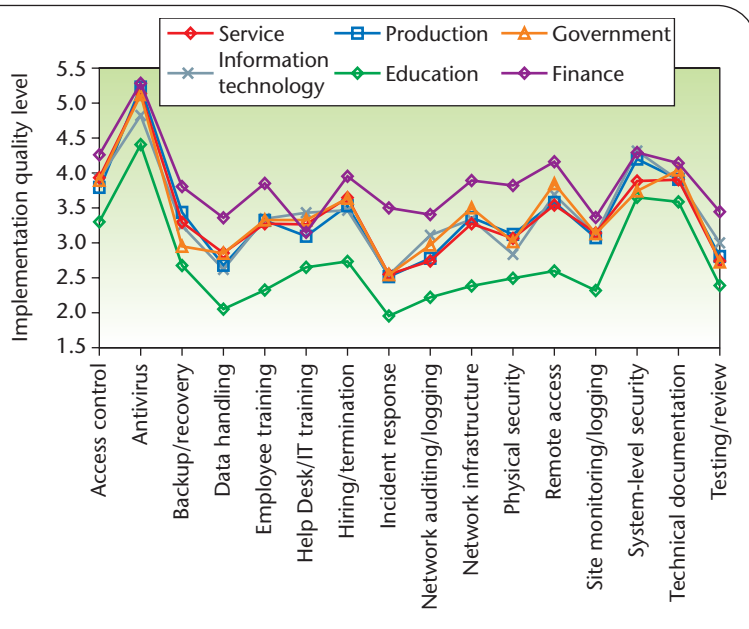


Figure 5. Control quality differences among industry groups.

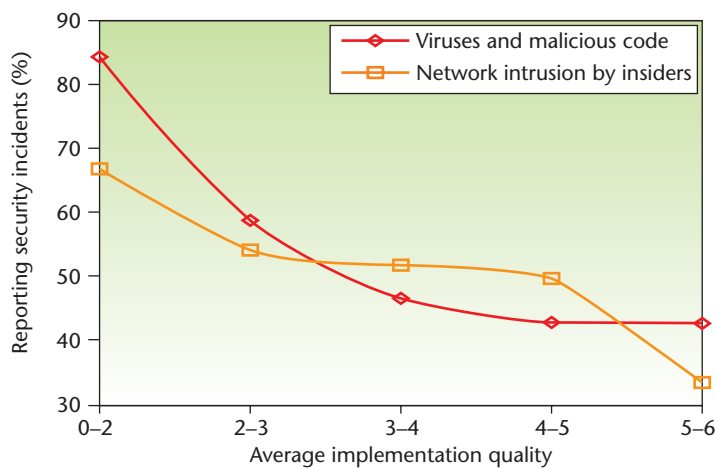


Figure 6. Incremental effect of program quality on reported security incidents.

tional effort or cost. Systems and compliance audits could look toward quality when assessing controls.

Future research should build on this approach and develop improved metrics of control strength and cost efficiency to optimize return on investment. Researchers should further investigate the benefits of combining various levels of technical, management, and operational controls to achieve true holistic security against a diverse range of present and future risks. Although our findings reveal some positive trends, organizations will need further progress before they truly have information security “under control.” □

References

- O.S. Saydjari, “Multilevel Security: Reprise,” *IEEE Security & Privacy*, vol. 2, no. 5, 2004, pp. 64–67.
- R.T. Mercuri, “Computer Security: Quality Rather than Quantity,” *Comm. ACM*, vol. 45, no. 10, 2002, pp. 12–14.
- D.W. Straub and R.J. Welke, “Coping with Systems Risk: Security Planning Models for Management Decision-Making,” *MIS Quarterly*, vol. 22, no. 4, 1998, pp. 441–470.
- G. Dhillon and J. Backhouse, “Information Systems Security Management in the New Millennium,” *Comm. ACM*, vol. 43, no. 7, 2000, pp. 125–128.
- G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems,” Nat’l Inst. of Standards and Technology, US Dept of Commerce, 2002; <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.
- L. Gordon et al., *Ninth Ann. CSI/FBI Computer Crime and Survey Report*, Computer Security Inst., 2004.
- M.E. Whitman, “Enemy at the Gate: Threats to Information Security,” *Comm. ACM*, vol. 46, no. 8, 2003, pp. 91–95.
- A.G. Kotulic and J.G. Clark, “Why There Aren’t More Information Security Research Studies,” *Information & Management*, vol. 41, 2004, pp. 597–607.
- M. Bishop, “What is Computer Security?” *IEEE Security & Privacy*, vol. 1, no. 1, 2003, pp. 67–69.
- T. Belchner et al., “Riptech Internet Security Threat Report,” *Riptech*, 2002.
- “The Internet Business Disruptions Benchmark Report,” Aberdeen Group, 2004; www.aberdeen.com/summary/report/benchmark/ibd.asp.
- L.A. Gordon and M.P. Loeb, “The Economics of Information Security Investment,” *ACM Trans. Information and System Security*, vol. 5, no. 4, 2002, pp. 438–457.
- A.V. Feigenbaum, “Total Quality Control,” *Harvard Business Rev.*, vol. 34, no. 6, 1956, p. 93.

Wade H. Baker is a PhD candidate in the Department of Business Information Technology at Virginia Tech and an information risk management consultant for Cybertrust. His research interests include information security, risk modeling and management, business intelligence, and decision support systems. Baker has an MS in information technology from the University of Southern Mississippi. He is a member of the Decision Sciences Institute, Institute for Operations Research and the Management Sciences (Informs), and the Anti-Phishing Working Group. Contact him at wade.baker@cybertrust.com.

Linda Wallace is an associate professor in the Department of Accounting and Information Systems at Virginia Tech. Her research interests include software project risk, agile software development, information security, and online communities. Wallace has a PhD in computer information systems from Georgia State University. She is a member of the special interest group on Information Systems of the Project Management Institute (PMI-ISSIG). Contact her at wallacel@vt.edu.