Nov 14th, 12:05 PM - 12:30 PM

Using Experts for Improving Project Cybersecurity Risk Scenarios

Steven S. Presley
University of South Alabama, ssp1521@jagmail.southalabama.edu

Jeffrey P. Landry
University of South Alabama, jlandry@southalabama.edu

Jordan Shropshire
University of South Alabama, jshropshire@southalabama.edu

Philip Menard
University of Texas at San Antonio, philip.menard@utsa.edu

Abstract

This study implemented an expert panel to assess the content validity of hypothetical scenarios to be used in a survey of cybersecurity risk across project meta-phases. Six out of 10 experts solicited completed the expert panel exercise. Results indicate that although experts often disagreed with each other and on the expected mapping of scenario to project meta-phase, the experts generally found risk present in the scenarios and across all three project meta-phases, as hypothesized.

Disciplines

Information Security | Management Information Systems

Comments

10-31 Update: Added ORCID for each author.

CCERP Paper 1153 - Using Experts for Improving Project Cybersecurity Risk Scenarios

Responses to Reviewer Recommendations and Feedback

Reviewer's issue

Our response

Report standard deviation along with means in table 3

As the sample size for this phase (5 or 6) was very small, calculating statistics was not useful or particularly meaningful, and so we refrained from calculating the standard deviations, and we say so in the paper now. We also added a limitations section that mentioned this, too.

The final study to be published in a future article had n=66 and we will report complete statistics including standard deviation and other measures of effect size. The stats reported here in table 3 are only meant to be interpreted as preliminary indicators that our scenarios were potentially useful for the final study, which was our goal for this phase.

Write in third person

We removed more than 30 occurrences of "we", "our" and "us", converting to third person voice

Add more literature review

We added references to:

- Studies about breaches or security issues related to project cybersecurity
- IS security papers that used hypothetical scenarios
- An additional expert panel paper

More detail on the instrument design—any additional assessments?

We wrote up more detail on the development of the instrument, including pilot studies before and after the expert panel.

Using Experts for Improving Project Cybersecurity Risk Scenarios

Steven S. Presley
Digital Industries Software
Siemens A.G.
Plano, TX
ssp1521@jagmail.southalabama.edu
ORCID: 0000-0003-0386-8983

Jeffrey P. Landry
School of Computing
University of South Alabama
Mobile, AL
jlandry@southalabama.edu
ORCID: 0000-0003-4144-601X

Jordan Shropshire
School of Computing
University of South Alabama
Mobile, AL
jshropshire@southalabama.edu
ORCID: 0000-0002-4177-8578

Phil Menard
UTSA Carlos Alvarez College of Business
University of Texas at San Antonio
San Antonio, TX
philip.menard@utsa.edu
ORCID: 0000-0001-8696-3198

***Abstract*—This study implemented an expert panel to assess the content validity of hypothetical scenarios to be used in a survey of cybersecurity risk across project meta-phases. Six out of 10 experts solicited completed the expert panel exercise. Results indicate that although experts often disagreed with each other and on the expected mapping of scenario to project meta-phase, the experts generally found risk present in the scenarios and across all three project meta-phases, as hypothesized.**

Keywords— Cybersecurity, Project risk, Risk Management, Survey research, Construct validity

I. Introduction

As part of an empirical study of project cybersecurity risk as it unfolds over time, the authors planned to survey project management and cybersecurity professionals. They developed a questionnaire comprised of 25 hypothetical scenarios. Each scenario paired a particular project asset with a cybersecurity threat and illustrated how that threat made the asset vulnerable. The scenarios were written at a concrete level with specific facts that experts in project management and cybersecurity would hopefully recognize and understand. Each scenario was written to illustrate a threat originating in one of the three temporal phases. As such, the use of a survey in this fashion constitutes a quasi-experimental design. The study sought to determine whether the scenarios would be useful and valid for assessing project cybersecurity risk. For assessing the survey, the authors enlisted the help of an expert panel. The purpose of this paper is to describe the use of this cybersecurity expert panel for reviewing and improving the scenario-based survey.

If successful, the scenario-based survey may then be used as part of a quasi-experimental research design for the co-authors' larger study. The larger study proposes to answer the question of whether and how much risk is perceived to be present throughout a project's temporal phases by project and cybersecurity personnel. It is hypothesized that risk may be introduced before projects begin, and may impact project deliverables and stakeholders long after project closeout. The results of the larger study may have implications for an organization's security management stance at different phases of the project's life span.

II. Literature Review

Three areas of study contribute to the development and review of the project cybersecurity scenarios and survey. The first area is project meta-phases, used in the larger study as a temporal framework around which risk can be estimated. The second area is risk analysis methodology, used to identify and assess risk. The third area is construct validity in the context of surveys that use hypothetical scenarios.

A. Project Meta-phases

A temporal model of project meta-phases [1] was established to describe the dynamic complexities involved in project management. These three project meta-phases established in the authors' framework are Project Conception (before the project begins), Project Execution (when the project officially begins and its deliverables are being implemented), and Deliverable Use (after project closeout and through the useful life of the project's deliverables). Project actors, artifacts, and activities change throughout a project's extended life span. For example, in the project conception meta-phase, the project sponsor is a prominent actor, project proposals are important artifacts, and project selection is a key activity. See Table I for examples of project meta-phase actors, artifacts, and activities.

Applied to cybersecurity, it may be important to understand the dynamics of the various meta-phases. Project assets, in their various forms and at different stages of development, may be subject to vulnerabilities that may be discovered at a later point in time. As part of a larger study, the authors of this paper seek to establish a baseline of project cybersecurity risk across the meta-phases.

The items in the authors' survey reflect risk scenarios across the three project meta-phases.

B. Risk Analysis

Organizations that engage in project management, particularly for the development and deployment of computer-based information systems, are subject to a wide variety of cybersecurity threats. Whitman's asset-based threat assessment approach [2] and [3] was selected for identifying potential cybersecurity threats. Whitman's framework consists of 12

categories of threats [2]. To identify risk, the threat-vulnerability-asset (TVA) analysis technique [3] was used. A list of project assets was identified using three sources of information: self-generated lists of actors, artifacts, and activities across the meta-phases; the components of information systems; and a review of literature pertaining to project-related cybersecurity incidents and security, such as [4], [5], [6], [7], [8], [9], and [10]. For the various assets, one or more threats from the Whitman framework were paired with the assets, creating threat-asset pairs.

Each T-A pair has an associated vulnerability for which, in a practical sense, the risk can be estimated and then treated by the organization with one of several possible risk response strategies. A list of 25 T-A pairs was identified. For example, one such T-A pair consists of the threat "deliberate acts of espionage or trespass" paired with the asset "business strategy information."

At first, the researchers created a set of questions based on the T-A pairs. However, an initial pilot study, consisting of the faculty members in cybersecurity in the doctoral student's department, demonstrated that the such an exercise was lengthy, and there was much uncertainty about the subjects' estimation of risk, given the abstractness of the T-A pairs. Hypothetical scenarios were then chose based on their containing more situation specific, salient information.

For each T-A pair, a hypothetical threat scenario was written. For the previous example, the scenario developed is "A foreign state-supported manufacturer compromised the servers of several major U.S. competitors, obtaining market research reports and strategic forecasts. The manufacturer used these to gain competitive advantages." Each scenario was written to illustrate the introduction of some cybersecurity risk in a project context, specific to one of three of the meta-phases. The above scenario was written for the Conception meta-phase. The scenarios became part of a questionnaire designed to estimate risk through items that assessed the probability and consequences of each scenario's occurrence.

The first set of 18 scenarios were then pilot tested with a group of 25 graduate students taking an information assurance course. About 8 or 9 students evaluated each scenario. Of the 25 students surveyed all but one found it easy to estimate risk and complete the survey. Moreover, the respondents believed risk was present in all 18 scenarios to some degree. As the use of scenarios seemed promising, seven more scenarios were written to provide broader coverage of assets and threats. A total of 25 scenarios had been written at this point.

C. Construct Validity

Hypothetical scenarios have several advantages. They may provide face validity through the practical implementation of abstract T-A pairs. Another advantage of hypothetical scenarios is that is that they are not subject to social desirability bias that might be present if they had to answer questions on their own organizational experiences. By presenting each respondent with a fresh, hypothetical scenario, the study is also free from recall bias that would result if the respondents had been asked to rely on a remembered past experience as the focal area. Hypothetical scenarios have been used in prior IS security research. One paper [11] described the use of hypothetical scenarios as a recognized methodology. Referred to as vignettes, their study coupled realistic scenarios and numerical ratings to study intent in security policy violations. Similar examples were found as well describing advantages to scenario-based surveys such as [12] and [13].

But a question remains as to the content validity of the scenarios used in the questionnaire. Taken together, are these scenarios useful and valid for estimating project cybersecurity risk? This is the central question of this paper. Content validity is "an assessment of how well a set of scale items matches with the relevant content domain of the construct that it is trying to measure" [14]. It is common to use expert judges in the domain of inquiry to assess content validity. Lawshe [15] established a quantitative test of content validity through the use of experts who voted on each of a construct item's usefulness/necessity for measuring the construct in question.

Since the scenarios are also treatments in a quasi-experiment, a question remains as to the internal validity of the design. As each scenario is written for a specific project meta-phase, a key independent variable in the larger study, it is also possible to test the scenarios using a manipulation check. A manipulation check is used to verify that research subjects can confirm the treatment they have received. While doing so may not always be necessary, manipulation checks may shed light on how subjects are interpreting the independent variable. A successful manipulation check may offset the potential for a confounding variable [16].

III. Research Proposition

The major proposition of this paper is now put to the test. This study proposes that a questionnaire consisting of 25 hypothetical project cybersecurity scenarios will be deemed useful to estimate risk, and across all three project meta-phases of conception, execution and deliverable use. Such an instrument, established to assess risk, will also have good content validity. To test the assertion of content validity, the methodology described in the next section was used.

IV. Methodology

The methodology chosen for this study is a survey of a panel of experts. A small panel of experts was chosen to review the authors' questionnaire on project cyber security risk. Ten experts were recruited for participation in the panel. Each of the experts was an experienced researcher in areas of cybersecurity who were colleagues of one member of the doctoral student's dissertation committee, but were not committee members themselves.

A. Survey Development

The panel was provided with a survey consisting of a set of instructions, and 25 "blocks" of scenario-based questions. Each block contained some questions that the respondents in the doctoral student's larger study would also receive, as well as questions intended just for the experts themselves. The respondent questions were the project cybersecurity scenario and questions about the risk implied by the scenario (one probability and one consequences question), as follows:

Question N.1 On a scale of 1 to 5, what are the potential consequences (e.g. damaged reputation, disrupted operations, or financial losses) to an organization should the above scenario occur?

0 - Not Applicable
1 - Negligible Consequences
2 - Minor Consequences
3 - Important Consequences
4 - Serious Consequences
5 - Very Serious Consequences

Question N.2 On a scale of 1 to 5, what is the relative probability that a similar scenario could occur?

0 - Not Applicable
1 - Very Low Probability
2 - Low Probability
3 - Medium Probability
4 - High Probability
5 - Very High Probability

The two questions intended for the reviewers only were a question asking them to map the scenario to one of three project meta-phases and a question asking them whether the scenario was useful [15] for inclusion in the survey. The question on the mapping to project meta-phase was for experts only, as was the usefulness question. The survey also included an optional, open-ended comments question on each scenario.

The wording of the meta-phase mapping question was as follows:

Question N.3 When are [assets in the scenario] first created, used or modified in a typical project?

1 - Project Conception (i.e., before the project officially begins)
2 - Project Execution (i.e., when the project is ongoing)
3 - Deliverable Use (i.e., after the project is over and deliverables are being used)
Not Applicable (i.e., this is not an asset for most projects)

The wording of the Lawshe-inspired question [15] was as follows:

Question N.4 Is the threat scenario....

- *Essential*
- *Useful but not essential*
- *Not necessary*

All ten experts were solicited. The survey was implemented in Qualtrics and sent to the experts via an email solicitation. One week later a reminder was sent. Of the ten experts originally contacted, five completed the survey completely, and a sixth completed half of the survey but also supplied a lengthy email with qualitative feedback. All expert input was used in the analysis.

V. Results

Four main issues arose from the expert review. Three of these were content or internal validity issues and the remaining one dealt with response rate and respondent fatigue. In summary, the issues were: (1) some scenarios were deemed by experts as "not useful"; (2) mapping scenarios to the correct project meta-phase was difficult, as experts disagreed; (3) some scenarios lacked enough detail for estimating risk; and (4) the survey was found to be too long. Each issue and the review decisions are discussed in the next four sub-sections.

A. Items Not Useful

One of the three content validity issues surfaced by experts was that of item usefulness. Not all of the 25 scenarios were found to be equally useful. In fact, some experts responded to the Lawshe question with the "not useful" decision. All ten of these scenarios were removed from the survey. This action served two purposes. It eliminated scenarios that experts deemed not useful, leaving only more useful ones. It also helped to shorten the survey. The list of scenarios receiving a "not useful" vote included these ten (wording shortened):

- sharing technical project specs with one's spouse, who works for a competitor
- spear-phishing a key project team member
- failure of PM team's mobile devices to trigger security updates
- failed backup procedure during a ransomware attack
- project delays due to a natural disaster
- using an obsolete component that later gets exploited
- notorious state-sponsor forcing a software maker to implement software back doors
- disgruntled key project person being hired away by a competitor
- stolen laptop with project data
- viral outbreak forcing quarantine of main project sponsor

These scenarios were re-read to interpret why they received a "not useful" vote. In most cases, it was likely because there was very little risk perceived by the expert. Either it was because the scenario was unlikely to occur or else would not result in significant consequences. In other cases, the scenario may have been too similar to another scenario. The viral outbreak scenario may have received its two "not useful" votes due to the salience of the coronavirus pandemic and a strong perception of the lack of its effect on projects. The perceived widespread success of remote working as well as the realization of the rarity of pandemics led them to rate the scenario as low risk.

B. Mapping to Project Meta-phase

The experts were asked to map threat scenarios to project meta-phase, but they rarely agreed. See Table II with results on meta-phase mapping. The scenarios included are the final 12—four for each meta-phase, that were included in the empirical survey to follow.

Only one of the scenarios was mapped by all experts as intended. The lowest level of agreement—see column Meta-phase Match %—was 33%. The average agreement across all scenarios was 70%.

The issues with non-agreement were believed to be ambiguity. Some of the scenarios were complex with issues of causation present in a different time then when the threat was being realized. Especially with respect to deployment-related risk, experts could interpret the threat either being part of project execution or part of deliverable use. Sometimes, assets mentioned, such as "production and delivery schedules", may have created ambiguity as they dealt with manufacturing assets rather than project assets. In another scenario, an email system was breached, resulting in project planning documents being exposed. But the reviewers may have thought that the vulnerable asset was the email system rather than the planning artifact. Scenarios were revised to remove ambiguity.

C. Lack of Risk-Related Detail

The expert who provided the qualitative feedback explained that several scenarios lacked risk-related detail. Specifically, he asked "what kind of system was breached?" or "what kinds of data are stored in that system?" or "what was the consequence of that vulnerability?" The lack of detail prevented him from specifying risk—consequence in particular. The authors improved these scenarios by adding details such as "customer information system" or "financial data".

See Table III containing the list of 12 scenarios. For each, the risk-related expert feedback is provided in columns Probability and Consequences. The mean values for probability and consequences for all three project meta-phases are also shown. Both probability and consequences were measured on a 5-point scale. Sample standard deviations were not calculated due to the small sample size not being useful for statistical comparisons. Examination of the raw data indicated patterns of agreement, however.

The highest probability and consequences of project cybersecurity threats were in the project execution meta-phase (3.29 and 3.88), followed by the deliverable use meta-phase, and then conception. Each meta-phase had at least one threat scenario rated at a level of 3.5 or better for probability and for consequences. That is a level between medium and high probability and between important and serious consequences.

D. Survey Too Long

Finally, the issue of survey length was addressed. One of the experts said that the survey took him one hour. The co-authors themselves agreed that it could take respondents about 45-minutes once the extra instructions and questions for experts were removed. Some guidance states that most respondents would prefer to take about 10-15 minutes maximum [14]. In the interest of response rate and preventing fatigue, the survey was shortened. The instructions were shortened to a bare minimum, including only the briefest of explanation and only that information required by the university's Institutional Review Board to inform and protect human subjects.

Exactly four scenarios were selected per meta-phase. In addition to the scenarios eliminated from experts rating them as "not useful", several others got eliminated. Not only did this decision help with a respondent satisfaction issue, but it created a more balanced set of scenarios. With equal splitting of scenarios across meta-phases, a possible confounding variable is eliminated. Should only one meta-phase be left, the level of risk at the project meta-phase, it is important to eliminate alternative explanations for why risk varies.

To test whether the changes to the scenarios made their meta-phase mapping clearer, another pilot study was conducted. A group of graduate students enrolled in a project and change management course were surveyed. They were given each scenario and questioned about the meta-phase. Despite the changes, there was still widespread disagreement about meta-phase. So, the scenarios were written to include explicit mentioning of the affected meta-phase, and the meta-phase question was to be used only as a manipulation check.

VI. Discussion

The qualitative feedback from the one expert was as valuable as the quantitative feedback from the whole group. He provided reasons why particular scenarios were difficult for risk assessment purposes. From his suggestions, the researchers were able to craft a rationale for modifying the remaining scenarios. The recommendation is that, when using experts, seek the open-ended feedback in addition to the quantitative feedback.

VII. Limitations

The major limitation of the expert panel review of the scenarios was in the balance of quantitative and qualitative feedback. The sample of experts was too small to make statistical tests useful. Note that sample standard deviations were not reported in Table 3. The qualitative feedback was quite useful, but came almost exclusively from one panelist. Perhaps a more qualitative approach such as recommended by [17] could have been used.

VIII. Conclusions and Future Directions

Feedback received during the expert panel review motivated the authors to improve the research design of a larger subsequent study by selecting the scenarios with generally positive feedback, revising them to improve phasal mapping and risk-identifiability, and shortening the questionnaire through elimination of less recognizable scenarios and providing more concise instructions for participants. Further testing of the scenarios was subsequently completed as part of the larger study [18] in which the perception of risk across meta-phases was present and measurable. It is believed that the refinement of the scenarios contributed considerably to the quality of the data received during the follow-on effort, the results of which are planned to be the subject of a future article.

References

[1] S. S. Presley, J. Landry, & J. Shropshire, "Three Meta-Phases of a Project," Proceedings of the Southern Association for Information Systems Conference, Atlanta, GA, USA March 23rd–24th, 2018.

[2] M. E. Whitman, "Enemy at the gate: threats to information security," Communications of the ACM, 46(8), 91-95. 2003.

[3] M. Whitman & H. Mattord, Management of Information Security, Fifth Edition. Boston, MA: CENGAGE Learning. 2016.

[4] C. Arthur, "Cyber-attack concerns raised over Boeing 787 chip's 'back door'," The Guardian.com, accessed from https://www.theguardian.com/technology/2012/may/29/cyber-attack-concerns-boeing-chip on May 14, 2021. May, 2012.

[5] Perez, E., & Wallace, G. "After Target breach, Homeland Security warns retailers," accessed from http://money.cnn.com/2014/01/16/news/companies/target-breach-report/index.html. Jan 16, 2014.

[6] C. Osborne, "InterContinental Hotels Group admits data breach," accessed from https://www.zdnet.com/article/intercontinental-hotels-group-admits-data-breach/. 2017.

[7] B. Miller, "Pandora's Power Grid – What Can State Attacks Do and What Would Be the Impact," Dartmouth College Institute for Security, Technology, and Society, online lecture, accessed from https://youtu.be/UDqaGlnLtNQ. May 2, 2017.

[8] N. Manworren, J. Letwat, & O. Daily, "Why you should care about the Target data breach," Elsevier: Business Horizons, 59, pp. 257—266. Doi: HTTP://dx.doi.org/10.1016/j.bushor.2016.01.002 . 2016.

[9] L. Esola, "Sony faces array of risks from hack," Business Insurance, 00076864 48(26) p. 0001 Dec. 22, 2014.

[10] C. Book, "Following Extortion Attempt, Gaming Network ESEA Breached, 1.5M Profiles Leaked," Threatpost.com, accessed from: https://threatpost.com/gaming-network-esea-breached-1-5m-profiles-leaked/122933/ Jan. 9, 2017.

[11] M. Siponen and A. Vance, "Neutralization: New insights into the problem of employee information systems security policy violations," MIS Quarterly 34(3):487-502. 2010.

[12] A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: An empirical study," MIS Quarterly 34(3), September:549-566. 2010.

[13] P. Menard, G. J. Bott, & R. E. Crossler, "User motivations in protecting information security: Protection motivation theory versus self-determination theory," Journal of Management Information Systems, 34(4), 1203-1230. 2017.

[14] A. Bhattacherjee, Social science research: Principles, methods, and practices, accessed from https://scholarcommons.usf.edu/oa_textbooks/3/ on May 4, 2021. Pps.77, 59. 2012.

[15] C. H. Lawshe, "A quantitative approach to content validity," Personnel psychology, 28(4), 563-575. 1975.

[16] D. J. Hauser, P. C. Ellsworth, & R. Gonzalez, "Are manipulation checks necessary?" Frontiers in psychology, 9, 998. 2018.

[17] D. R. Tojib & L. F. Sugianto, "Content Validity of Instruments in IS Research," Journal of Information Technology Theory and Application (JITTA), 8:3, 31-56. 2006.

[18] S. S. Presley, "Effective Cybersecurity Risk Management in Projects," University of South Alabama, Theses and Dissertations. 60. https://jagworks.southalabama.edu/theses_diss/60. 2022.

TABLE I. PROJECT ASSETS BY META-PHASE

Project asset → Project meta-phase	**Actors**	**Artifacts**	**Activities**
Project Concepts	Project sponsor, steering committee	Project proposals, plans, budgets	Project selection, planning
Project Execution	Project manager, project team, third party contractors	Legacy code, materials	Resource acquisition, product development, testing
Deliverable Use	Deployment team, maintenance and support staff, customers	Deliverables, production system	Deliverable deployment, ongoing maintenance

TABLE II. META-PHASE MAPPING RESULTS

S#	**Scenario (short description)**	**Votes for Conception /Execution /Deliverable Use**	**Intended Meta-phase**	**Meta-phase Score**	**Meta-phase Match %**
1	Movie studio's email breach of its movie scripts	6/0/0	Conception	6	100%
8	Breach of manufacturing schedules to a foreign competitor	3/1/2	Conception	3	50%
23	Firewall breach of DoD sensitive project planning documents to a rival state	3/1/1	Conception	3	60%
25	Hard drive failure results in loss of detail project justification analyses and reports	5/0/0	Conception	5	100%
11	Social engineering attack on third-party vendor for unauthorized access of production server	0/1/5	Deliverable Use	5	83%
17	A hotel chain's phased rollout leads to hacker exploitation of unprotected reservation system before security installed	1/1/3	Deliverable Use	3	60%
3	Hackers installed malware on an unprotected server during a system deployment	2/2/2	Deliverable Use	2	33%
13	A cyber-physical system used integrated circuits considered safe, but had back-doors that were exploited later	0/3/2	Deliverable Use	2	40%
4	A contractor accidentally installs malware that compromises a retail store's point of sale system	1/5/0	Execution	5	83%
6	Hackers exploited legacy code vulnerabilities in defense contract project	1/5/0	Execution	5	83%
2	A DoD agency recalled missile systems in the field that used faulty chips that had been acquired without proper inspection	0/4/2	Execution	4	67%
5	Student interns access a legacy database during a project and are exposed to sensitive student data that should remain private	1/4/0	Execution	4	80%

TABLE III. PERCEIVED RISK RESULTS BY SCENARIO

Short Scenario Description (meta-phase)	Probability	Meta-phase Probability Mean	Consequences	Meta-phase Consequences Mean
Conception Meta-phase		***2.89***		***3.39***
Movie studio's email breach of its movie scripts (conception)	3.5		3.83	
Breach of manufacturing schedules to a foreign competitor (conception)	3.67		3.33	
Firewall breach of DoD sensitive project planning documents to a rival state. (conception)	2.4		3.8	
Hard drive failure results in loss of detail project justification analyses and reports. (conception)	2		2.6	
Deliverable Use Meta-phase		***3.08***		***3.61***
Social engineering attack on third-party vendor for unauthorized access of production server. (deliverable use)	3		3.33	
A hotel chain's phased rollout leads to hacker exploitation of unprotected reservation system before security installed. (deliverable use)	3		3.4	
Hackers installed malware on an unprotected server during a system deployment (deliverable use)	3.5		3.5	
A cyber-physical system used integrated circuits considered safe, but had back-doors that were exploited later (deliverable use)	2.8		4.2	
Execution Meta-phase		***3.29***		***3.88***
A contractor accidentally installs malware that compromises a retail store's point of sale system. (execution)	4		4.17	
Hackers exploited legacy code vulnerabilities in defense contract project. (execution)	3.17		3.83	
A DoD agency recalled missile systems from the field that used faulty chips that had been acquired without proper inspection. (execution)	3		4.5	
Student interns access a legacy database during a project and are exposed to sensitive student data that should remain private. (execution)	3		3	