Asllani, Arben; Lari, Alireza; Lari, Nasim

Article

Strengthening information technology security through the failure modes and effects analysis approach

International Journal of Quality Innovation

Provided in Cooperation with:
Springer Nature

Suggested Citation: Asllani, Arben; Lari, Alireza; Lari, Nasim (2018) : Strengthening information technology security through the failure modes and effects analysis approach, International Journal of Quality Innovation, ISSN 2363-7021, Springer, Heidelberg, Vol. 4, Iss. 1, pp. 1-22, https://doi.org/10.1186/s40887-018-0025-1

Asllani et al. International Journal of Quality Innovation (2018) 4:5
https://doi.org/10.1186/s40887-018-0025-1

International Journal of Quality Innovation

EMPIRICAL ARTICLE Open Access

Strengthening information technology security through the failure modes and effects analysis approach

Arben Asllani[1*], Alireza Lari[2] and Nasim Lari[3]

* Correspondence: beni-asllani@utc.edu
[1]Rollins College of Business, University of Tennessee at Chattanooga, 615 McCallie Ave., Chattanooga, TN 37403, USA
Full list of author information is available at the end of the article

Abstract

Proper protection of information systems is a major quality issue of organizational risk management. Risk management is a process whereby risk factors are identified and then virtually eliminated. Failure modes and effects analysis (FMEA) is a risk management methodology for identifying system's failure modes with their effects and causes. FMEA identifies potential weaknesses in the system. This approach allows companies to correct areas identified through the process before the system fails. In this paper, we identify several critical failure factors that may jeopardize the security of information systems. In doing this, we systematically identify, analyze, and document the possible failure modes and the possible effects of each failure on the system. The proposed cybersecurity FMEA (C-FMEA) process results in a detailed description of how failures influence the system's performance and how they can be avoided. The applicability of the proposed C-FMEA is illustrated with an example from a regional airport.

Keywords: Information technology security, FMEA, Airport security, Quality management

Background

As companies introduce new technologies such as big data, cloud, and Internet of Things (IoT) to their work environment, security issues become more important. Cybersecurity professionals use all the tools to secure access to their networks and applications, while this protection is no longer enough. The digital transformation leads to an explosion of connected environments, and attackers will compromise weak links.

In an article by Roberts and Lashinsky in Fortune [1], the latest statistics are a call to arms: "According to Cisco, the number of so-called distributed denial-of-service (DDos) attacks – assaults that flood a system's servers with junk web traffic – jumped globally by 172% in 2016. Cisco projects that total to grow by another two and a half time, to 3.1 million attacks, by 2021." Considering the importance of secure information systems, the National Institute of Standards and Technology (US Department of Commerce—NIST) has developed security controls [2] for information systems in federal, private, and public organizations. NIST has also developed general guidelines [3], for federal government [4] and for non-government organizations [5], for managing the risk of information technology systems. Current controls and guidelines mostly

assume that the appropriate protection of the information systems security lies in risk management, where risk factors are identified and then gradually eliminated.

Most of the risk management practices in cybersecurity relate to compliance requirements, which force organizations to focus on security controls and vulnerabilities. Risk management considers multiple facets including assets, threats, vulnerabilities, and controls. A functionally integrated cybersecurity organization places the threats at forefront of strategic, tactical, and operational practices.

With all the new innovative applications of the Internet, there are opportunities to develop new products and services with new quality definitions that move away from the conventional utilitarian focus and became a factor of changing environment and competitive systems [6]. The security of Internet and in general the cybersecurity is now a quality matter and requires new quality assurance tools and methods. This paper introduces failure modes and effects analysis (FMEA) as a quality and reliability approach (FMEA) to assess, monitor, and mitigate cybersecurity threats.

FMEA is a method of reliability analysis intended to identify failure affecting the functioning of a system and enable priorities for action to be set. FMEA was first used in the defense industry in the 1940s for military products and is formalized in that industry in the Department of Defense's Military Standards Mil-Std-1629A. In the 1950s, parallel to Juran and Feignbaun's work, the US Department of Defense formed an ad hoc group on reliability of electronic equipment. This group strove to predict the failure rate of equipment. The group realized that prediction was not sufficient and developed an FMEA approach to reduce failure rates over time [7].

FMEA is a systematic group of activities intended to (a) recognize and evaluate the potential failure of a product or process and the effects of that failure, (b) identify actions that could eliminate or reduce the chance of the potential failure occurring, and (c) document the entire process. The rest of the paper is organized as follows. The section "Literature review" presents a review of the relevant literature on FMEA and its applications, its advantages as an approach to cybersecurity, and its effectiveness, and a brief discussion of using FMEA to assess information systems threats and risk as a security tool. In the section "Using FMEA for risk assessment and cybersecurity," the authors present the theoretical foundation and the development of the model with a discussion of information security and how confidentiality, integrity, and availability can be viewed as quality matters, together with the proposed methodology and specific steps for implementing FMEA for cybersecurity. A hypothetical example of an airport is presented to demonstrate the implementation of FMEA to mitigate the risk of cybersecurity threats. Finally, the conclusions offer a roadmap for other organizations that want to implement FMEA to better secure their information systems and related issues.

Literature review

Failure modes and effects analysis (FMEA) is frequently used in product design to identify the most critical causes of a product's failure and to mitigate those risks. Since 1980, military standards (MIL-STD-1629A) have considered information security as a quality issue and have recommended the use of FMEA to monitor threats and other failure causes [8]. FMEA can be used in major business areas including concept (to analyze a system in the conception of the design), process (to analyze the assembly and manufacturing processes), design (to analyze the products before mass production

starts), service (to test industry processes for failure prior to their release to customers), and equipment (to analyze equipment before the final purchase).

In practice, FMEA is a qualitative assessment of risk that relies on the judgment of experts. In many cases, it is difficult to replicate the analysis and this makes it a static and case-based model. In practice, FMEA is performed in structured sessions by a team of expert analysts. The quality of the outcome depends on the ability of the analysts to predict the ways in which components might fail and how the system will behave in the presence of such failures.

FMEA is used in manufacturing, service, administrative processes, and recently in information technology and security. Table 1 summarizes a small sample of the contexts where FMEA has been applied.

Both Avaram [17] and Shirouyehzad et al. [12] agree that having a risk management strategy can lead to a successful implementation of enterprise resource planning (ERP) systems. FMEA provides more reliability in the system and can reduce the need for modifications to the design, provide product improvement on a continual basis, and reduce manufacturing costs. Most recently, Muckin and Fitch [13] of Lockheed Martin Corporation offer a "threat-driven" approach to cybersecurity and recommend using FMEA to monitor the security of an information system. Also, Silva et al. [14] and Ayofe and Irwin [18] use FMEA to analyze the security threats.

In other applications, Mandal and Maiti [15] use FMEA for risk analysis and Patel et al. [11] offer a method to quantify risk in terms of a numeric value or degree of cybersecurity. Zafar et al. [16] consider security as a matter of quality and propose a quality model to enhance software security. They use a quality framework, originally proposed by Dromey [9], to identify known security defects, their fixes, and the underlying low-level software components along with the properties that positively influence the overall security of the product. The International Electro-technical Commission (IEC) provides the standard IEC 60812, a document that provides a forward search that identifies consequences of already identified failure modes using FMEA. There is also a backward search process to identify all the relevant causes for each hazard; a commonly used technique is fault tree analysis (FTA), presented in IEC 61025.

The aerospace industry introduced FMEA in the 1960s which is used extensively by Six Sigma practitioners to quantify and prioritize risk within a process, product, or system and then track actions to mitigate that risk [22]. Chrysler, Ford, and GM first published the common FMEA reference manual in 1993 following the discussions during the 1988 ASQ Automotive Division conference, which was extensively used for design and processes. FMEA is also used to improve the safety of drug delivery, to improve health care facility design, for the formulation of pediatric parenteral nutrition solution,

Table 1 Application areas of FMEA

Application areas	Literature source
Information systems	[9–18]
Space, aircraft, and avionics	[19–22]
Automotive industry	[23, 24]
Health care	[25–28]
Food industry	[29]
Military	[30]

and to reduce errors in processes. In the application related to military operations, Grunske et al. [30] introduced a model checker to automate the search for system-level consequences of component failure. The idea is to inject runtime faults into a model based on the system specification and check if the resulting model violates safety requirements, specified as temporal logical formulas. This enables the safety engineer to identify if a component failure, or combination of multiple failures, can lead to a specified hazard condition. If so, the model checker produces an example of the events leading up to the hazard occurrence which the analyst can use to identify the relevant failure propagation pathways and co-effectors. The process is applied on three medium-sized case studies modeled with Behavior Trees.

Different sources, including the American Society for Quality, explained the FMEA methodology and the steps [7, 31]. These steps are:

1) Identify different functions of the system that should be performed and where the potential of failure exists. The system may need to be decomposed in order to better identify the risks, and later, an integration is expected.
2) For each function, identify potential risks/failure modes to describe how a function may fail to be performed.
3) Describe what happens for each failure mode especially the effects perceived by the user or operator. The effects should carefully be measured so the severity of each effect can be judged.
4) Categorize how severe each hazard will be. In FMEA literature, there are four different types of hazards: catastrophic, critical, marginal, and negligible. It could be also rated on a scale of 1 to 10 (1 for insignificant and 10 being catastrophic).
5) Estimate the relative chance or probability of each failure to happen. A 10-point scale can estimate the likelihood from highly unlikely (1) to very likely (10).
6) Estimate the ease of failure detection. If the detection of failure takes too long, it may become late to repair the situation and the magnitude of the problem will become much greater.
7) Calculate the risk priority number (RPN) for each risk/failure and analyze risks using a Pareto distribution.
8) Decide what action to take in order to eliminate or reduce the highest risks in the system.
9) Reassess risks with another cycle of FMEA.

Methods

The proposed cybersecurity FMEA (C-FMEA) methodology evaluates the quality of the information system security in terms of confidentiality, integrity, and availability (CIA) triad and intends to improve the reliability of security measures, recommend and record appropriate actions to mitigate the threats, and improve the efficiency and reduce the cost of cybersecurity [32, 33].

Theoretical development/model—proposed C-FMEA approach

While in this methodology, the authors follow the general FMEA steps suggested by ASQ [31], the core of discussion is on the identification of failure modes and taking

corrective actions based on CIA triad. For this purpose, the quality standard of *confidentiality* and privacy aims to protect data from being viewed or disclosed to unauthorized parties. One of the confidentiality principles is to provide access to data and information only to authorized individuals with a defined and specific need to see or use that information. Some of the possible failure modes regarding confidentiality include disclosing data to unauthorized parties, collecting unauthorized information about customers, anonymizing or masking sensitive data, illegal intrusion to data and information, not locking files properly, not removing identifiers from questionnaires or electronic data files, or not encrypting files containing identifiers [34]. Each of these confidentiality failure modes can be avoided by proper defensive actions. For example, cryptography and encryption methods are to ensure the confidential transmission of data from one computer or system to another. Cryptography hides or codes the information as it is being transmitted on a network, and encryption ensures that unauthorized users do not read data since only those who hold the encryption key can decrypt the information.

The quality standard of *integrity* of information technology (IT) systems aims to guarantee that the information is modified and destroyed only by authorized parties, is modified and destroyed only in authorized ways, and is assumed to be authentic, (i.e., authorized parties can be verified), and any change of information cannot be repudiated (i.e., cannot be denied by the authorized changing party). There exist several measures to provide end-to-end data integrity. These measures include installation of antivirus programs, establishing authenticity and non-repudiation protocols, applying "check--sum" procedures, and installation of system and data recovery utility software programs. Malware is a common root cause of data corruption, and it can cause intentional or unintentional loss of data integrity. A virus also alters files and renders an information system unusable. A "check-sum" procedure can be used to detect and correct possible data corruption. Other programs can repair the corrupted file automatically, depending on the level of corruption. In more extreme cases, when data seems to be uncorrectable, one can apply automatic restoration from backups.

The quality standard of *availability* aims to make data and information available to the authorized users when it is needed. Very often, data is time-sensitive and the value may diminish if delayed. A typical failure mode for availability of a system occurs when access to the information is delayed or denied due to denial-of-service attacks, power outages, floods, fires, or other environmental or man-made disasters. The best corrective actions to ensure data availability are regular data backups, off-site data storage, redundant parallel systems, and physical protection of information systems.

In the proposed C-FMEA methodology, the authors recommend adding a responsibility matrix, which maps the actions or controls to the assigned people responsible for implementation of such controls. FMEA is an iterative approach, and as actions are completed, the team must record the results and modify the values of S, O, and D. In this section, the FMEA approach is intuitively attuned to mitigate the cybersecurity threats. The Cyber RPN (CRPN), in such a case, is a product of the cyber threat impact (in a scale from 1 to 10), the chance that the cyber threat will happen (in a scale of 1 to 10), and the chance that the cyber threat can be detected (also in a scale of 1 to 10). CRPN can be used to generate corrective actions and to set cyber threat goals and assure that these goals are achieved with appropriate cyber defensive strategies.

We use FMEA to incorporate security issues into the design of an IT system. The required steps that will be explained in details with the case presented in the next section.

Results and Discussion

Information systems have become the driving force of the airport infrastructure. Such heavy dependency of airport operations on hardware, software, data, and networks has a dual and opposing impact on airport security: while the technology has become beneficial to enhance the security of airport operations, at the same time, it poses vulnerabilities to potential cyber-attacks [35]. For example, the common use of terminal equipment (CUTE) is an IT-driven system that allows several airlines to share gates and check-in counters. However, sharing CUTE among several airlines, while increasing efficiency and lowering the cost, causes security concerns when airlines share data, protocols, procedures, and information. These concerns are related to firewalls, passwords, intrusion protection, and operational security [36]. C-FMEA methodology demonstrates the ability to address these concerns and enhance the security of information systems.

Creating a team of experts to implement C-FMEA is the prerequisite for a successful implementation. The system administrator or other information technology personnel are responsible for implementing security measures, and as such, they must initiate and lead the C-FMEA project. However, it is suggested that end-users of the information systems should participate in the systems security projects. We can use FMEA to design an IT system in which the security issues are incorporated. To do so, we need to follow these steps:

1) Identify components of an information system.

Decompose the information technology system design process into smaller components in a way that you can reintegrate to get the total system in mind. Give each component of the system design a unique identifier, so that a decomposition of the system can later end to a complete integration and no component is overlooked. This can be done through preparation of a work breakdown structure (WBS) chart. Identifying the components of the information systems at the airport helps to decide which aspects of the airport security are most vulnerable to physical break-ins or unauthorized use. Typical components of an airport network as related to security are security processes, policies and procedures, people, digital devices connected to the network, network components, and physical locations that the components are located.

2) For each component or subsystem, list all the necessary functions and all the expectations that are in mind. In other words, we introduce some performance measures and expectations from each component that when put together gives a flawless and secure total system. We are defining processes and procedures that are necessary to ensure confidentiality, integrity, and availability of data and information.

Figure 1 illustrates the list of processes and procedures related to an airport network security. Each of the processes listed in Fig. 1, when fail to be implemented properly, is

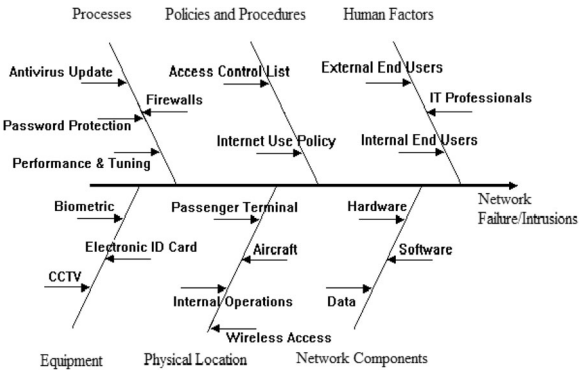

Fig. 1 List of processes and procedures to ensure CIA

a potential source for network vulnerability. In the *process* category, there are four causes of security threats: antivirus software not updated, passwords not changed periodically, fireworks are misplaced, and the security administrator has not completed performance testing and tuning periodically. The security *policies and procedures* must also be followed to avoid possible network failures, unwanted intrusions, and threat of CIA. There are three categories of people in the *human factor* component involved in the airport network security. The first category is passengers, including external end-users operating in the check-in and boarding areas. The second category is the airport security personnel and airline employees, also known as internal end-users. The third category is IT personnel. C-FMEA approach considers any member of these groups as a potential cause that can jeopardize the security of the network, either unintentionally or intentionally.

The *equipment* component lists several network devices that physically secure the airport operations. Examples of these devices include electronic ID cards, closed circuit TVs, or biometric measurement devices. When used improperly, the network security devices can jeopardize the security of the airport network. Figure 1 also identifies major causes of network security breach related to *physical locations*. These areas include the area around the gates and aircraft, the terminal, the internal operation zone, and the back office. Finally, each *network component* is a potential cause for security intrusion or failure.

3) For each function and process, list potential failure modes as they relate to CIA triad. This means we identify ways that the system may malfunction and go wrong. Describe what happens for each failure modes especially the effect perceived by the user or operator. If that component does not perform as it should, what would be the effect?

Table 2 indicates potential failure modes for each network security process at the airport as related to the three components of security. For this exercise, the authors have indicated one or more failures based on the general understanding of airport security matters. Each airport network has its own specifics, and the team created for each C-FMEA project identifies the failure modes.

4) For each process, identify the responsibilities of person(s) in charge of correcting failure mode for each process.

Table 2 Failure modes as related to the CIA triad

Security processes	Failure modes		
	Confidentiality	Availability	Integrity
Antivirus update			x
Firewall		x	
Password protection	x		
Performance and tuning			x
Access control list	x	x	
Internet use policy	x		x
External users	x		x
Internal users	x		x
IT professionals			x
CCTV	x		
Biometric	x		
Electronic ID cards	x		
Terminal		x	
Aircraft			x
Wireless access		x	x
Internal operations			x
Hardware	x	x	x
Software	x	x	x
Data	x	x	x

Table 3 shows a summary of these responsibilities. Antivirus updates must be performed by everyone in the organization, and firewall protection must be established by the airport IT professionals and network administrators. Internal users must always change their passwords, and network administrator must set password requirements and enforce them continuously. IT professionals, database administrators, and network administrators must ensure that the IT network performs at its full capacity and is always up-to-date with the latest software releases. Database and network administrators review the access control list (ACL) and formulate and enforce end-user and Internet access policies while internal users are responsible for implementing such policy.

IT professionals, database and network administrators, and airport security personnel must enforce security practices and monitor the compliance with such practices of external and internal users, as well as IT professionals at the airport. Secure performance of closed circuit cameras, biometric devices, and electronic ID cards are the responsibility of network administrator and the airport security. Airport security and airline employees must enforce proper access to terminal and aircraft. Network administrator must allow a secure access to the wireless network while the security of IT-enhanced internal operations is the responsibility of internal users, IT professionals, database and network administrators, and airport security personnel. The network security administrator and other IT personnel must address the potential attacks on hardware and software. Finally, unauthorized access to databases is the responsibility of the database administrator.

Table 3 Mapping security processes with security personnel

Security processes	Internal users	IT professionals	Database administrator	Network administrator	Airport security
Antivirus update	X	x	x	x	x
Firewall		x		x	
Password protection	X			x	
Performance and Tuning		x	x	x	
Access control list			x	x	
Internet use policy	X	x		x	
External users		x	x	x	x
Internal users		x	x	x	x
IT professionals		x	x	x	
CCTV				x	x
Biometric				x	x
Electronic ID cards				x	x
Terminal	X				x
Aircraft	X				x
Wireless access				x	
Internal operations	X	x		x	x
Hardware		x		x	
Software		x		x	
Data			x	x	

5) Estimate the severity (S) of the effects for each failure using a 10-point scale. In FMEA literature, there are four different types of hazards: catastrophic, critical, marginal, and negligible.

In a typical risk analysis, the ranking of severity is based on the estimated cost to address or repair a security failure. However, in practice, it is difficult to estimate such losses especially when there is no data from previous security breaches. The C-FMEA approach recommends a more practical approach: using the team of experts to estimate a severity score in a scale from 1 to 10. An old but relevant structured communication technique, known as the Delphi method [37], can be successfully used by the C-FMEA team to estimate the values of *S* for each failure mode. Severity values for each security process are shown in the second column (*S*) of Table 4.

6) Estimate the relative chance of each failure to occur (O) using a 10-point scale from unlikely (1) to very likely (10).

Security experts and the C-FMEA team can also estimate the likelihood that a failure will occur. For lack of prior experience, we also recommend the use of the Delphi method. The chance of occurrence for each failure can also be revised in lieu of any news or intelligence reports on potential security threats. The estimated values of the chance of occurrence are shown in the third column (*O*) of Table 4.

7) Estimate the ease with which the failure may be detected (D) using a 10-point scale. If the detection of failure takes long, then it may become too late to repair and magnitude of the problem is to be much greater than if the failure can be easily detected.

A similar approach as in steps 5 and 6 (Delphi method, team's expertise, cyber intelligence reports) can be used to estimate the degree of detecting a cybersecurity attack. Table 4 shows the values in the fourth column (D).

8) Estimate the highest risk process as the maximum of $\{S \times O \times D\}$ for each process.

The cyber risk priority number (CRPN) is calculated by multiplying the severity (S), occurrence (O), and detection (D), and the results are shown in the fifth column of Table 4.

9) Decide what action is to be taken to eliminate or reduce the highest risk and use the responsibility matrix from step 4 to assign responsibility and take actions.

Ghosh [38] recommends taking corrective actions for any process or component with CRPN value exceeding 80. The corrective action ideally leads to a lower CRPN number. Once the priorities are calculated, a detailed plan of action can be generated. The information systems components and each potential failure mode are listed with its CRPN number in Table 5. For example, firewall updates, password protection measures, the Internet use policy enforcements, internal operations security reviews, antivirus updates, biometric devices security, and wireless security are considered significant threats

Table 4 Calculating CRPN for each security failure at the network

Failure causes	*S*	*O*	*D*	CRPN
Antivirus update	3	5	6	90
Firewall	7	3	4	84
Performance and tuning	2	7	5	70
Password protection	4	7	3	84
Access control list	5	2	8	80
Internet use policy	6	2	7	84
Internal users	3	6	4	72
IT professionals	2	4	5	40
CCTV	3	2	6	36
Biometric	3	4	8	96
Electronic ID cards	2	3	4	24
Terminal	3	3	1	9
Aircraft	3	3	1	9
Internal operations	3	7	4	84
Wireless access	4	8	3	96
Hardware	2	4	4	32
Software	2	2	3	12
Data	3	4	6	72

Table 5 Action plan recommended by C-FMEA project

IS component	Failure causes	CRPN	Person responsible
Processes	Antivirus update	90	Internal users
			IT professionals
			Network administrators
	Firewall	84	IT professionals
			Network administrators
	Performance and tuning	70	IT professionals
			Database administrators
			Network administrators
	Password protection	84	Internal users
			Network administrators
Policies and procedures	Access control list	80	Database administrators
			Network administrators
	Internet use policy	84	Internal users
			IT professionals
			Network administrators
Human factors	Internal users	72	IT professionals
			Database administrators
			Network administrators
			Airport security
	IT professionals	40	IT professionals
			Database administrators
			Network administrators
Equipment	CCTV	36	Network administrators
			Airport security
	Biometric	96	Network administrators
			Airport security
	Electronic ID cards	24	Network administrators
			Airport security
Physical location	Terminal	9	IT professionals
			Airport security
	Aircraft	9	IT professionals
			Airport security
	Internal operations	84	Internal users
			IT professionals
			Network administrators
			Airport security
Network component	Wireless access	96	Network administrator
	Hardware	32	IT professionals
			Network administrators
	Software	12	IT professionals
			Network administrators
	Data	72	Database administrators
			Network administrators

(CRPN > 80), and as such, priority dates are assigned to deal with these threats. For each action, details about start date, completion date, and responsible parties are provided.

At this stage of the C-FMEA project, the responsible party implements specific security measures to address the causes of failure. Such actions include random security controls, or updating the digital devices such as scanners, metal detectors, and backscatter X-rays [39].

With the execution of operational plan, the new set of values for *S*, *O*, and *D* are calculated and a new list of recommendations for future actions is prepared. Implementation of the C-FMEA project provides insights and lessons for the airport security administrators. For example, the network administrator can generate guidelines about training procedures, improve Internet use policy, and revise security measures for physical protection of the network facilities.

Conclusions

This paper offers a unique approach to managing the security of the information systems. The proposed C-FMEA methodology has several advantages compared to traditional risk management approaches. The main thrust of the paper is considering security as a quality matter, (i.e., a high-quality information system is the one that processes, communicates, and produces data with a high level of confidentiality, integrity, and availability). The proposed methodology incorporates these three dimensions of IT security into the traditional FMEA approach already used in manufacturing or service systems. The process of protecting the organizational networks and their information systems is a continuous process, and the authors propose the C-FMEA process as a continuous project. System administrators and consultants can use the approach to analyze any vulnerability in an existing information system and to offer proactive recommendations to protect the system against potential threats.

The proposed C-FMEA is a qualitative and systematic tool, typically created within a spreadsheet, to help practitioners anticipate the things might go wrong with an information system in general or its components. In addition to determining how an information system might fail, C-FMEA also helps find the possible causes of failures and the likelihood of failures before their occurrence. The ability to anticipate security issues early allows cybersecurity administrators to prevent potential failures or vulnerabilities. The authors demonstrated the proposed methodology using a hypothetical example. This was a learning exercise, and the authors intend to implement the methodology in a real case environment.

Abbreviations

ACL: Access control list; ASQ: American Society for Quality; C-FMEA: Cybersecurity FMEA; CIA: Confidentiality, integrity, and availability; CRPN: Cyber RPN; CUTE: Common use of terminal equipment; *D*: Detection; DDos: Distributed denial-of-service; ERP: Enterprise resource planning; FMEA: Failure modes and effects analysis; FTA: Fault tree analysis; IEC: International Electro-technical Commission; IT: Information technology; MIL-STD-1629A: Military standards; NIST: National Institute of Standards and Technology; *O*: Occurrence; RPN: Risk priority number; *S*: Severity; WBS: Work breakdown structure

Availability of data and materials

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Authors' contributions

AA offered his expertise on cybersecurity, AL offered his quality management background, and NL contributed to the overall literature review. All the three authors equally participated in the writing and editing of the manuscript. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1]Rollins College of Business, University of Tennessee at Chattanooga, 615 McCallie Ave., Chattanooga, TN 37403, USA. [2]School of Business, Wake Forest University, P.O. Box 7285, Winston-Salem, NC 27109, USA. [3]IBM, 600 14th Street NW #300, Washington, DC 20005, USA.

Received: 29 August 2018 Accepted: 25 September 2018
Published online: 08 October 2018

References

1. Roberts J, Lashinsky A (2017) Business under assault from cybercriminals like never before, and the cost to companies is exploding, *Fortune*, p 54
2. NIST (2013) Security controls for federal information systems and organizations. (Special publication 800-53, revision 4). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, Accessed 29 Dec 2016, from National Institute of Standards and Technology
3. NIST (2002) Risk management guide for information technology systems (special publication 800-30). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, Accessed 29 Dec 2016, from National Institute of Standards and Technology
4. NIST (2006) Guide for developing security plans for federal information systems. (Special publication 800-18). https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01, Accessed 21 Dec 2016, from National Institute of Standards and Technology
5. NIST (2011) Managing information security risk. (Special publication 800-39). http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf, Accessed 3 Jan 2017, from National Institute of Standards and Technology
6. Lee SM (2015) The age of quality innovation. Int J Qual Innov. https://doi.org/10.1186/s40887-015-0002-x
7. Stamatis DH (1995) Failure mode and effect analysis, FMEA from theory to execution. Quality Press, Milwaukee
8. US Department of Defense (1980) Military standard 1629A. Retrieved January 5, 2017, from US Department of Defense: http://www.fmea-fmeca.com/milstd1629.pdf
9. Dromey RG (1995) A model for software product quality. IEEE Trans Softw Eng 21(2):146–162
10. Zhang Y, Zhu H, Greenwood S, Huo Q (2001) Quality modeling for web-based information systems. Proceedings of 8th IEEE Workshop on Future Trends of Distributed Computing Systems, pp 41–47
11. Patel SC, Graham JH, Ralston PA (2008) Quantitatively assessing the vulnerability of critical information systems: a new method for evaluating security enhancements. Int J Inf Manag 28(6):483–491
12. Shirouyehzad H, Dabestani R, Badakhshian M (2011) The FMEA approach to identification of critical failure factors in ERP implementation. Int Bus Res 4(3):254–263. https://doi.org/10.5539/ibr.v4n3p254
13. Muckin M, Fitch, S C (2014) A threat-driven approach to cybersecurity. https://pdfs.semanticscholar.org/be09/f7a16eb4a379e698d8f42100fd8a91943a0c.pdf, Accessed 5 Jan 2017, from Lockheed Martin Corporation
14. Silva MM, Gusmão AP, Poleto T, Silva LC, Costa AP (2014) A multidimensional approach to information security risk management using FMEA and fuzzy theory. Int J Inf Manag 34(6):733–740
15. Mandal S, Maiti J (2014) Risk analysis using FMEA: fuzzy similarity value and possibility theory based approach. Expert Syst Appl 41:3527–3537
16. Zafar S, Mehboob M, Naveed A, Malik B (2015) Security quality model: an extension of Dromey's model. Softw Qual J 23:29–54
17. Avaram C D (2010) ERP inside Large Organizations. Informatica Economica 14(4), 196–208
18. Ayofe A, Irwi B (2010) Cybersecurity: challenges and the way forward. Comput Sci Telecommun 29(6):56–69
19. Garrick BJ (1988) The approach to risk analysis in three industries: nuclear power, space systems, and chemical process. Reliab Eng Syst Saf 23(3):195–205
20. Murphy EE (1989) Aging aircraft: too old to fly? IEEE Spectr 26(6):28–31
21. Pari G, Kumar S, Sharma V (2008) Reliability improvement of electronic standby display system of modern aircraft. Int J Qual Reliab Manag 25(9):955–967
22. Foster TS (2007) Managing quality: integrating the supply chain (5th ed.). Prentice Hall, New Jersey
23. SAE (1995) SAE 1739 – potential failure mode and effects analysis in design (design FMEA), potential failure mode and effects analysis in manufacturing and assembly processes (process FMEA)
24. AIAG (2008) AIAG FMEA-4: potential failure mode and effect analysis (FMEA), 4th edn. The Automotive Division of the American Society for Quality (ASQC) and the Automotive Industry Action Group (AIAG), Southfield
25. DeRosier J, Stalhandske E, Baigan JP, Nudell T (2002) Using health care failure node and effect analysis: the VA National Center for Patient Safety's prospective risk analysis system. Jt Comm J Qual Improv 28(5):248–267
26. Apkon M, Leonard J, Probst L, Delizio L, Vitale R (2004) Design of a safer approach to intravenous drug infusion: failure mode effects analysis. Qual Saf Health Care 13(4):265–271
27. Reiling JG, Knutzen BL, Stoecklein M (2003) FMEA – the cure for medical errors. Qual Prog 36(8):67–71

28. Bonnabry P, Cingra L, Sadeghipour FH, Fonzo-Christe C, Pfister R (2015) Use of a systematic risk analysis method to improve safety in the production of pediatric parenteral nutrition solution. Qual Saf Health Care 14(2):93–98
29. Sciponi A, Saccarola G, Centazzo A, Arena F (2002) FMEA methodology design, implementation and integration with HACCP system in a food company. Food Control 13(8):495–501
30. Grunske L, Winter K, Yatapanage N, Zafar S, Lindsay P (2011) Experience with fault injection experiments for FMEA. Wiley Online Library, pp 1233–1258. https://doi.org/10.1002/spe.1039
31. ASQ (2016) Failure mode effects analysis (FMEA). http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html, Accessed 14 Jan 2017, from ASQ Web site
32. Perrin C (2008) The CIA Triad. http://www.techrepublic.com/blog/it-security/the-cia-triad/ Accessed 6 Jan 2017 from IT Security
33. Gibson D (2011) Understanding the security triad (confidentiality, integrity, and availability). http://www.pearsonitcertification.com/articles/article.aspx?p=1708668, Accessed 6 Jan 2017, from Pearson IT certification
34. National Research Council (2005) Risks of access: potential confidentiality breaches and their consequences. In: Panel on data access for research purposes, expanding access to research data: reconciling risks and opportunities. The National Academies Press, Washington, D. C, pp 50–62
35. Asllani A, Ali A (2011) Securing information systems in airports: a practical approach. Proceedings of the 6th International Conference for Internet Technology and Secured Transactions, pp 314–318
36. Feldman J (2003) First-class IT service. Netw Comput 14(7):44–49
37. Dalkey N, Helmer O (1963) An experimental application of the DELPHI method to the use of experts. Manag Sci 9(3), 458–467
38. Ghosh M (2010) Process failure mode effects analysis (PFMEA). http://www.processexcellencenetwork.com/business-process-management-bpm/articles/process-failure-mode-effects-analysis-pfmea, Accessed 5 Jan 2017, from Process Excellence Network
39. Holbrook E (2010) Airport security: privacy vs. safety, risk management, 57 (2), 12–14