Influential Article Review - Reinforcing IT Defense Thru Failure Modes

Drew Scott

Kenneth Hardy

This paper examines information technology. We present insights from a highly influential paper. Here are the highlights from this paper: 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. For our overseas readers, we then present the insights from this paper in Spanish, French, Portuguese, and German.

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

SUMMARY

- 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 . For example, the common use of terminal equipment 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 . 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.

- 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.
- Failure modes as related to the CIA triad. 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.
- Mapping security processes with security personnel. 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.
- Calculating CRPN for each security failure at the network. The cyber risk priority number is calculated by multiplying the severity , occurrence , and detection , and the results are shown in the fifth column of Table 4.
- 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.
- Action plan recommended by C-FMEA project. 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 .

HIGHLY INFLUENTIAL ARTICLE

We used the following article as a basis of our evaluation:

Asllani, A., Lari, A., & Lari, N. (2018). Strengthening information technology security through the failure modes and effects analysis approach. International Journal of Quality Innovation, 4(1), 1–14.

This is the link to the publisher's website:
https://jqualityinnovation.springeropen.com/articles/10.1186/s40887-018-0025-1

INTRODUCTION

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 the 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 become a factor of changing environment and competitive systems [6]. The security of the Internet and in general 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.

CONCLUSION

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 that 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.

APPENDIX

FIGURE 1
LIST OF PROCESSES AND PROCEDURES TO ENSURE CIA

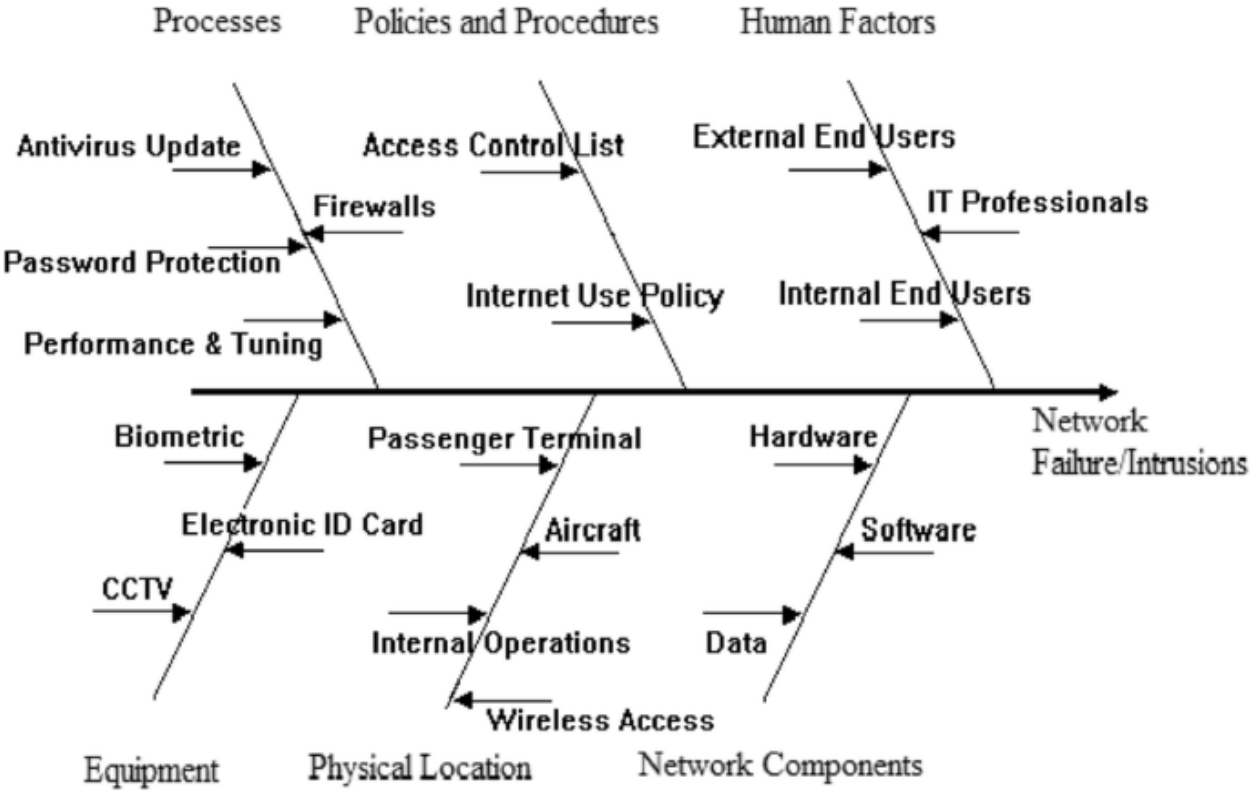

TABLE 1
APPLICATION AREAS OF FMEA

Application areas	**Literature source**
Information systems	[10,11,12,13,14,15,16,17,18]
Space, aircraft, and avionics	[19,20,21,22]
Automotive industry	[23, 24]
Health care	[25,26,27,28]
Food industry	[29]
Military	[30]

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
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	

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

REFERENCES

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

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

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

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

Avaram C D (2010) ERP inside Large Organizations. Informatica Economica 14(4), 196–208

Ayofe A, Irwi B (2010) Cybersecurity: challenges and the way forward. Comput Sci Telecommun 29(6):56–69

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

Dalkey N, Helmer O (1963) An experimental application of the DELPHI method to the use of experts. Manag Sci 9(3), 458–467

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

Dromey RG (1995) A model for software product quality. IEEE Trans Softw Eng 21(2):146–162

Feldman J (2003) First-class IT service. Netw Comput 14(7):44–49

Foster TS (2007) Managing quality: integrating the supply chain (5th ed.). Prentice Hall, New Jersey

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

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

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
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
Holbrook E (2010) Airport security: privacy vs. safety, risk management, 57 (2), 12–14
Lee SM (2015) The age of quality innovation. Int J Qual Innov. https://doi.org/10.1186/s40887-015-0002-x
Mandal S, Maiti J (2014) Risk analysis using FMEA: fuzzy similarity value and possibility theory based approach. Expert Syst Appl 41:3527–3537
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
Murphy EE (1989) Aging aircraft: too old to fly? IEEE Spectr 26(6):28–31
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
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
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
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
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
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
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
Perrin C (2008) The CIA Triad. http://www.techrepublic.com/blog/it-security/the-cia-triad/ Accessed 6 Jan 2017 from IT Security
Reiling JG, Knutzen BL, Stoecklein M (2003) FMEA – the cure for medical errors. Qual Prog 36(8):67–71
Roberts J, Lashinsky A (2017) Business under assault from cybercriminals like never before, and the cost to companies is exploding, Fortune, p 54
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)
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
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
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
Stamatis DH (1995) Failure mode and effect analysis, FMEA from theory to execution. Quality Press, Milwaukee

US Department of Defense (1980) Military standard 1629A. Retrieved January 5, 2017, from US Department of Defense: http://www.fmea-fmeca.com/milstd1629.pdf
Zafar S, Mehboob M, Naveed A, Malik B (2015) Security quality model: an extension of Dromey's model. Softw Qual J 23:29–54
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

TRANSLATED VERSION: SPANISH

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSION TRADUCIDA: ESPAÑOL

A continuación se muestra una traducción aproximada de las ideas presentadas anteriormente. Esto se hizo para dar una comprensión general de las ideas presentadas en el documento. Por favor, disculpe cualquier error gramatical y no responsabilite a los autores originales de estos errores.

INTRODUCCIÓN

A medida que las empresas introducen nuevas tecnologías como big data, la nube y el Internet de las cosas (iot) en su entorno de trabajo, los problemas de seguridad se vuelven más importantes. Los profesionales de la ciberseguridad utilizan todas las herramientas para proteger el acceso a sus redes y aplicaciones, mientras que esta protección ya no es suficiente. La transformación digital conduce a una explosión de entornos conectados, y los atacantes pondrán en peligro los vínculos débiles.

En un artículo de Roberts y Lashinsky en Fortune [1], las últimas estadísticas son una llamada a las armas: "Según Cisco, el número de ataques de denegación de servicio distribuidos (ddos) – asaltos que inundan los servidores de un sistema con tráfico web basura – saltó globalmente en 172% en 2016. Cisco proyecta que el total crecerá otros dos tiempos y medio, a 3,1 millones de ataques, para 2021." Teniendo en cuenta la importancia de los sistemas de información seguros, el Instituto Nacional de Estándares y Tecnología (Departamento de Comercio de los Estados Unidos—NIST) ha desarrollado controles de seguridad [2] para los sistemas de información en organizaciones federales, privadas y públicas. El NIST también ha elaborado directrices generales [3], para el gobierno federal [4] y para organizaciones no gubernamentales [5], para gestionar el riesgo de los sistemas de tecnología de la información. Los controles y directrices actuales asumen principalmente que la protección adecuada de la seguridad de los sistemas de información reside en la gestión de riesgos, donde los factores de riesgo se identifican y luego eliminan gradualmente.

La mayoría de las prácticas de gestión de riesgos en ciberseguridad se relacionan con los requisitos de cumplimiento, que obligan a las organizaciones a centrarse en los controles de seguridad y vulnerabilidades. La administración de riesgos considera varias facetas, incluidos activos, amenazas, vulnerabilidades y controles. Una organización de ciberseguridad integrada funcionalmente pone las amenazas a la vanguardia de las prácticas estratégicas, tácticas y operativas.

Con todas las nuevas aplicaciones innovadoras de Internet, existen oportunidades para desarrollar nuevos productos y servicios con nuevas definiciones de calidad que se alejan del enfoque utilitario convencional y se convirtieron en un factor de entorno cambiante y sistemas competitivos [6]. La seguridad de Internet y, en general, de la ciberseguridad es ahora un asunto de calidad y requiere nuevas herramientas y métodos de garantía de calidad. Este documento introduce los modos de falla y el análisis de efectos (FMEA) como un enfoque de calidad y confiabilidad (FMEA) para evaluar, monitorear y mitigar las amenazas de ciberseguridad.

FMEA es un método de análisis de fiabilidad destinado a identificar fallas que afectan al funcionamiento de un sistema y permitir que se establezcan prioridades de acción. FMEA fue utilizado por primera vez en la industria de defensa en la década de 1940 para productos militares y se formaliza en esa industria en las Normas Militares Mil-Std-1629A del Departamento de Defensa. En la década de 1950, paralelamente al trabajo de Juran y Feignbaun, el Departamento de Defensa de los Estados Unidos formó un grupo ad hoc sobre la confiabilidad de los equipos electrónicos. Este grupo se esforzó por predecir la tasa de fallas de los equipos. El grupo se dio cuenta de que la predicción no era suficiente y desarrolló un enfoque FMEA para reducir las tasas de fallas a lo largo del tiempo [7].

FMEA es un grupo sistemático de actividades destinadas a (a) reconocer y evaluar el posible fallo de un producto o proceso y los efectos de ese fallo, (b) identificar acciones que podrían eliminar o reducir la posibilidad de que se produzca la falla potencial, y (c) documentar todo el proceso. El resto del documento se organiza de la siguiente manera. La sección "Revisión de la literatura" presenta una revisión de la literatura pertinente sobre FMEA y sus aplicaciones, sus ventajas como un enfoque de la ciberseguridad, y su eficacia, y una breve discusión sobre el uso de FMEA para evaluar las amenazas de los sistemas de información y el riesgo como una herramienta de seguridad. En la sección "Uso de FMEA para la evaluación de riesgos y la ciberseguridad", los autores presentan los fundamentos teóricos y el desarrollo del modelo con una discusión sobre la seguridad de la información y cómo la confidencialidad, integridad y disponibilidad pueden ser vistas como cuestiones de calidad, junto con la metodología propuesta y los pasos específicos para implementar FMEA para la ciberseguridad. Se presenta un ejemplo hipotético de un aeropuerto para demostrar la implementación de FMEA para mitigar el riesgo de amenazas de ciberseguridad. Por último, las conclusiones ofrecen una hoja de ruta para otras organizaciones que desean implementar FMEA para asegurar mejor sus sistemas de información y cuestiones relacionadas.

CONCLUSIÓN

Este documento ofrece un enfoque único para gestionar la seguridad de los sistemas de información. La metodología C-FMEA propuesta tiene varias ventajas en comparación con los enfoques tradicionales de gestión de riesgos. El objetivo principal del documento es considerar la seguridad como un asunto de calidad, (es decir, un sistema de información de alta calidad es el que procesa, comunica y produce datos con un alto nivel de confidencialidad, integridad y disponibilidad). La metodología propuesta incorpora estas tres dimensiones de la seguridad de TI en el enfoque tradicional de FMEA ya utilizado en los sistemas de fabricación o de servicio. El proceso de protección de las redes organizativas y sus sistemas de información es un proceso continuo, y los autores proponen el proceso C-FMEA como un proyecto continuo. Los administradores y consultores del sistema pueden utilizar el enfoque para analizar cualquier vulnerabilidad en un sistema de información existente y ofrecer recomendaciones proactivas para proteger el sistema contra posibles amenazas.

La C-FMEA propuesta es una herramienta cualitativa y sistemática, típicamente creada dentro de una hoja de cálculo, para ayudar a los profesionales a anticipar las cosas podrían salir mal con un sistema de información en general o sus componentes. Además de determinar cómo un sistema de información puede fallar, C-FMEA también ayuda a encontrar las posibles causas de fallas y la probabilidad de fallas antes de su ocurrencia. La capacidad de anticiparse a tiempo de los problemas de seguridad permite a los administradores de ciberseguridad prevenir posibles errores o vulnerabilidades. Los autores demostraron la metodología propuesta utilizando un ejemplo hipotético. Este fue un ejercicio de aprendizaje, y los autores tienen la intención de implementar la metodología en un entorno de caso real.

TRANSLATED VERSION: FRENCH

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSION TRADUITE: FRANÇAIS

Voici une traduction approximative des idées présentées ci-dessus. Cela a été fait pour donner une compréhension générale des idées présentées dans le document. Veuillez excuser toutes les erreurs grammaticales et ne pas tenir les auteurs originaux responsables de ces erreurs.

INTRODUCTION

À mesure que les entreprises introduisent de nouvelles technologies telles que le Big Data, le cloud et l'Internet des objets (iot) dans leur environnement de travail, les questions de sécurité deviennent plus importantes. Les professionnels de la cybersécurité utilisent tous les outils pour sécuriser l'accès à leurs réseaux et applications, alors que cette protection ne suffit plus. La transformation numérique conduit à une explosion d'environnements connectés, et les attaquants compromettront les maillons faibles.

Dans un article de Roberts et Lashinsky in Fortune [1], les dernières statistiques sont un appel aux armes : « Selon Cisco, le nombre d'attaques dites de déni de service distribué (ddos) – les agressions qui inondent les serveurs d'un système de trafic web indésirable – a bondi à l'échelle mondiale de 172 % en 2016. Cisco prévoit que le total augmentera de deux ans et demi, pour atteindre 3,1 millions d'attaques d'ici 2021. Compte tenu de l'importance de la sécurité des systèmes d'information, le National Institute of Standards and Technology (US Department of Commerce—NIST) a mis au point des contrôles de sécurité [2] pour les systèmes d'information dans les organisations fédérales, privées et publiques. Le NIST a également élaboré des lignes directrices générales [3], pour le gouvernement fédéral [4] et pour les organisations non gouvernementales [5], pour la gestion du risque des systèmes de technologie de l'information. Les contrôles et les lignes directrices actuels supposent principalement que la protection appropriée de la sécurité des systèmes d'information réside dans la gestion des risques, où les facteurs de risque sont identifiés puis éliminés progressivement.

La plupart des pratiques de gestion des risques en matière de cybersécurité sont liées aux exigences de conformité, qui obligent les organisations à se concentrer sur les contrôles de sécurité et les vulnérabilités. La gestion des risques tient compte de multiples aspects, notamment les actifs, les menaces, les vulnérabilités et les contrôles. Une organisation de cybersécurité fonctionnellement intégrée place les menaces à l'avant-garde des pratiques stratégiques, tactiques et opérationnelles.

Avec toutes les nouvelles applications novatrices d'Internet, il existe des possibilités de développer de nouveaux produits et services avec de nouvelles définitions de qualité qui s'éloignent de l'orientation utilitaire conventionnelle et sont devenus un facteur de l'évolution de l'environnement et des systèmes concurrentiels [6]. La sécurité d'Internet et, en général, la cybersécurité est désormais une question de qualité et nécessite de nouveaux outils et méthodes d'assurance de la qualité. Ce document présente les modes de défaillance et l'analyse des effets (FMEA) comme une approche de qualité et de fiabilité (FMEA) pour évaluer, surveiller et atténuer les menaces de cybersécurité.

La FMEA est une méthode d'analyse de fiabilité destinée à identifier les défaillances affectant le fonctionnement d'un système et à définir les priorités d'action. FMEA a été utilisé pour la première fois dans l'industrie de la défense dans les années 1940 pour les produits militaires et est formalisé dans cette industrie dans les normes militaires du ministère de la Défense Mil-Std-1629A. Dans les années 1950, parallèlement aux travaux de Juran et Feignbau, le département américain de la Défense a formé un groupe ad hoc sur la fiabilité des équipements électroniques. Ce groupe s'est efforcé de prédire le taux de défaillance de l'équipement. Le groupe s'est rendu compte que la prévision n'était pas suffisante et a élaboré une approche de la FMEA pour réduire les taux d'échec au fil du temps [7].

La FMEA est un groupe systématique d'activités visant à a) reconnaître et évaluer l'échec potentiel d'un produit ou d'un processus et les effets de cette défaillance, b) identifier les actions qui pourraient éliminer ou réduire les risques d'échec potentiel, et c) documenter l'ensemble du processus. Le reste du document est organisé comme suit. La section « Examen de la littérature » présente un examen de la documentation pertinente sur la FMEA et ses applications, ses avantages en tant qu'approche de la cybersécurité, et son efficacité, et une brève discussion sur l'utilisation de la FMEA pour évaluer les

menaces et les risques des systèmes d'information comme outil de sécurité. Dans la section « Utilisation de la FMEA pour l'évaluation des risques et la cybersécurité », les auteurs présentent la base théorique et l'élaboration du modèle avec une discussion sur la sécurité de l'information et la façon dont la confidentialité, l'intégrité et la disponibilité peuvent être considérées comme des questions de qualité, ainsi que la méthodologie proposée et les étapes spécifiques pour la mise en œuvre de la FMEA pour la cybersécurité. Un exemple hypothétique d'un aéroport est présenté pour démontrer la mise en œuvre de la FMEA afin d'atténuer le risque de menaces de cybersécurité. Enfin, les conclusions offrent une feuille de route pour d'autres organisations qui souhaitent mettre en œuvre la FMEA afin de mieux sécuriser leurs systèmes d'information et les questions connexes.

CONCLUSION

Ce document offre une approche unique de la gestion de la sécurité des systèmes d'information. La méthode proposée de la C-FMEA présente plusieurs avantages par rapport aux approches traditionnelles de gestion des risques. L'objectif principal du document est d'envisager la sécurité comme une question de qualité (c.-à-d. Qu'un système d'information de haute qualité est celui qui traite, communique et produit des données avec un haut niveau de confidentialité, d'intégrité et de disponibilité). La méthodologie proposée intègre ces trois dimensions de la sécurité informatique dans l'approche traditionnelle de la FMEA déjà utilisée dans les systèmes de fabrication ou de service. Le processus de protection des réseaux organisationnels et de leurs systèmes d'information est un processus continu, et les auteurs proposent le processus C-FMEA comme un projet continu. Les administrateurs et les consultants du système peuvent utiliser cette approche pour analyser toute vulnérabilité dans un système d'information existant et pour proposer des recommandations proactives afin de protéger le système contre les menaces potentielles.

Le projet de C-FMEA est un outil qualitatif et systématique, généralement créé dans une feuille de calcul, pour aider les praticiens à anticiper les choses qui pourraient mal tourner avec un système d'information en général ou ses composantes. En plus de déterminer comment un système d'information pourrait échouer, C-FMEA aide également à trouver les causes possibles des défaillances et la probabilité de défaillances avant leur apparition. La capacité d'anticiper rapidement les problèmes de sécurité permet aux administrateurs de cybersécurité de prévenir d'éventuelles défaillances ou vulnérabilités. Les auteurs ont démontré la méthodologie proposée à l'aide d'un exemple hypothétique. Il s'agissait d'un exercice d'apprentissage, et les auteurs ont l'intention de mettre en œuvre la méthodologie dans un environnement de cas réel.

TRANSLATED VERSION: GERMAN

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

ÜBERSETZTE VERSION: DEUTSCH

Hier ist eine ungefähre Übersetzung der oben vorgestellten Ideen. Dies wurde getan, um ein allgemeines Verständnis der in dem Dokument vorgestellten Ideen zu vermitteln. Bitte entschuldigen Sie alle grammatikalischen Fehler und machen Sie die ursprünglichen Autoren nicht für diese Fehler verantwortlich.

EINLEITUNG

Wenn Unternehmen neue Technologien wie Big Data, Cloud und Internet of Things (iot) in ihre Arbeitsumgebung einführen, werden Sicherheitsfragen immer wichtiger. Cybersicherheitsexperten nutzen alle Tools, um den Zugriff auf ihre Netzwerke und Anwendungen zu sichern, während dieser Schutz nicht

mehr ausreicht. Die digitale Transformation führt zu einer Explosion vernetzter Umgebungen, und Angreifer werden schwache Verbindungen kompromittieren.

In einem Artikel von Roberts und Lashinsky in Fortune [1] sind die neuesten Statistiken ein Aufruf zu Waffen: "Laut Cisco ist die Zahl der so genannten Distributed Denial-of-Service (ddos)-Angriffe – Angriffe, die die Server eines Systems mit Junk-Web-Traffic überschwemmen – 2016 weltweit um 172% gestiegen. Cisco rechnet damit, dass bis 2021 weitere zweieinhalb Mal auf 3,1 Millionen Angriffe anwachsen werden." Angesichts der Bedeutung sicherer Informationssysteme hat das National Institute of Standards and Technology (US Department of Commerce– NIST) Sicherheitskontrollen [2] für Informationssysteme in föderalen, privaten und öffentlichen Organisationen entwickelt. NIST hat auch allgemeine Leitlinien [3] für die Bundesregierung [4] und für Nichtregierungsorganisationen [5] für das Management des Risikos von IT-Systemen entwickelt. Aktuelle Kontrollen und Richtlinien gehen meist davon aus, dass der angemessene Schutz der Sicherheit der Informationssysteme im Risikomanagement liegt, wo Risikofaktoren identifiziert und dann schrittweise beseitigt werden.

Die meisten Risikomanagementpraktiken in der Cybersicherheit beziehen sich auf Compliance-Anforderungen, die Unternehmen zwingen, sich auf Sicherheitskontrollen und Schwachstellen zu konzentrieren. Das Risikomanagement berücksichtigt mehrere Facetten, einschließlich Assets, Bedrohungen, Schwachstellen und Kontrollen. Eine funktional integrierte Cybersicherheitsorganisation stellt die Bedrohungen in den Vordergrund strategischer, taktischer und operativer Praktiken.

Mit all den neuen innovativen Anwendungen des Internets gibt es Möglichkeiten, neue Produkte und Dienstleistungen mit neuen Qualitätsdefinitionen zu entwickeln, die sich von der konventionellen utilitaristischen Ausrichtung entfernen und zu einem Faktor für sich verändernde Umwelt- und Wettbewerbssysteme wurden [6]. Die Sicherheit des Internets und generell die Cybersicherheit ist heute eine Qualitätsfrage und erfordert neue Qualitätssicherungsinstrumente und -methoden. In diesem Dokument werden Fehlermodi und Effektanalysen (FMEA) als Qualitäts- und Zuverlässigkeitsansatz (FMEA) zur Bewertung, Überwachung und Minderung von Cybersicherheitsbedrohungen eingeführt.

FMEA ist eine Methode der Zuverlässigkeitsanalyse, mit der Fehler identifiziert werden sollen, die das Funktionieren eines Systems beeinträchtigen, und es ermöglicht, Prioritäten für Maßnahmen festzulegen. FMEA wurde erstmals in den 1940er Jahren in der Verteidigungsindustrie für militärische Produkte eingesetzt und ist in dieser Branche in den militärischen Standards mil-Std-1629A des Verteidigungsministeriums formalisiert. In den 1950er Jahren bildete das US-Verteidigungsministerium parallel zu Juranund und Feignbaun eine Ad-hoc-Gruppe zur Zuverlässigkeit elektronischer Geräte. Diese Gruppe bemühte sich, die Ausfallrate der Ausrüstung vorherzusagen. Die Gruppe erkannte, dass die Vorhersage nicht ausreichte, und entwickelte einen FMEA-Ansatz, um die Ausfallraten im Laufe der Zeit zu reduzieren [7].

FMEA ist eine systematische Gruppe von Aktivitäten, die darauf abzielen, (a) das potenzielle Versagen eines Produkts oder Prozesses und die Auswirkungen dieses Ausfalls zu erkennen und zu bewerten, (b) Maßnahmen zu identifizieren, die das Auftreten des potenziellen Ausfalls beseitigen oder verringern könnten, und c) den gesamten Prozess zu dokumentieren. Der Rest des Papiers ist wie folgt organisiert. Der Abschnitt "Literaturrezension" präsentiert einen Überblick über die einschlägige Literatur über FMEA und seine Anwendungen, ihre Vorteile als Ansatz für Cybersicherheit und ihre Wirksamkeit sowie eine kurze Diskussion über die Verwendung von FMEA zur Bewertung von Bedrohungen und Risiken von Informationssystemen als Sicherheitsinstrument. Im Abschnitt "Verwenden von FMEA für Risikobewertung und Cybersicherheit" stellen die Autoren die theoretische Grundlage und die Entwicklung des Modells mit einer Diskussion über Informationssicherheit und wie Vertraulichkeit, Integrität und Verfügbarkeit als Qualitätsfragen betrachtet werden können, zusammen mit der vorgeschlagenen Methodik und spezifischen Schritten für die Implementierung von FMEA für Cybersicherheit. Ein hypothetisches Beispiel für einen Flughafen wird vorgestellt, um die Implementierung von FMEA zu demonstrieren, um das Risiko von Cybersicherheitsbedrohungen zu mindern. Schließlich bieten die Schlussfolgerungen eine Roadmap für andere Organisationen, die FMEA implementieren wollen, um ihre Informationssysteme und damit zusammenhängende Probleme besser zu sichern.

SCHLUSSFOLGERUNG

Dieses Dokument bietet einen einzigartigen Ansatz für die Verwaltung der Sicherheit der Informationssysteme. Die vorgeschlagene C-FMEA-Methodik hat gegenüber herkömmlichen Risikomanagementansätzen mehrere Vorteile. Das Hauptanliegen des Papiers ist die Berücksichtigung der Sicherheit als eine Frage der Qualität (d. H., ein hochwertiges Informationssystem ist dasjen, das Daten mit einem hohen Maß an Vertraulichkeit, Integrität und Verfügbarkeit verarbeitet, kommuniziert und produziert). Die vorgeschlagene Methodik integriert diese drei Dimensionen der IT-Sicherheit in den traditionellen FMEA-Ansatz, der bereits in Fertigungs- oder Dienstleistungssystemen verwendet wird. Der Prozess des Schutzes der Organisationsnetzwerke und ihrer Informationssysteme ist ein kontinuierlicher Prozess, und die Autoren schlagen den C-FMEA-Prozess als kontinuierliches Projekt vor. Systemadministratoren und Berater können den Ansatz verwenden, um Schwachstellen in einem vorhandenen Informationssystem zu analysieren und proaktive Empfehlungen zum Schutz des Systems vor potenziellen Bedrohungen zu geben.

Das vorgeschlagene C-FMEA ist ein qualitatives und systematisches Werkzeug, das in der Regel in einer Kalkulationstabelle erstellt wird, um Praktikern zu helfen, zu antizipieren, dass die Dinge mit einem Informationssystem im Allgemeinen oder seinen Komponenten schief gehen könnten. C-FMEA bestimmt nicht nur, wie ein Informationssystem ausfallen könnte, sondern hilft auch dabei, die möglichen Ursachen von Fehlern und die Wahrscheinlichkeit von Ausfällen vor dem Auftreten zu ermitteln. Die Möglichkeit, Sicherheitsprobleme frühzeitig zu antizipieren, ermöglicht es Cybersicherheitsadministratoren, potenzielle Ausfälle oder Schwachstellen zu verhindern. Die Autoren demonstrierten die vorgeschlagene Methodik anhand eines hypothetischen Beispiels. Dies war eine Lernübung, und die Autoren beabsichtigen, die Methodik in einer realen Fallumgebung umzusetzen.

TRANSLATED VERSION: PORTUGUESE

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSÃO TRADUZIDA: PORTUGUÊS

Aqui está uma tradução aproximada das ideias acima apresentadas. Isto foi feito para dar uma compreensão geral das ideias apresentadas no documento. Por favor, desculpe todos os erros gramaticais e não responsacule os autores originais responsáveis por estes erros.

INTRODUÇÃO

À medida que as empresas introduzem novas tecnologias como big data, nuvem e Internet das Coisas (iot) ao seu ambiente de trabalho, as questões de segurança se tornam mais importantes. Os profissionais de cibersegurança usam todas as ferramentas para garantir o acesso às suas redes e aplicativos, enquanto essa proteção não é mais suficiente. A transformação digital leva a uma explosão de ambientes conectados, e os atacantes comprometerão elos fracos.

Em um artigo de Roberts e Lashinsky na Fortune [1], as estatísticas mais recentes são um chamado às armas: "De acordo com a Cisco, o número de ataques chamados de negação de serviço distribuído (ddos) – assaltos que inundam os servidores de um sistema com tráfego de lixo na web – saltou globalmente em 172% em 2016. A Cisco projeta que esse total cresça por mais dois tempos e meio, para 3,1 milhões de ataques, até 2021." Considerando a importância de sistemas de informação seguros, o Instituto Nacional de Padrões e Tecnologia (NIST) desenvolveu controles de segurança [2] para sistemas de informação em organizações federais, privadas e públicas. A NIST também desenvolveu diretrizes gerais [3], para o governo federal [4] e para organizações não governamentais [5], para a gestão do risco de sistemas de

tecnologia da informação. Os controles e diretrizes atuais assumem principalmente que a proteção adequada da segurança dos sistemas de informação está na gestão de riscos, onde os fatores de risco são identificados e, em seguida, gradualmente eliminados.

A maioria das práticas de gerenciamento de riscos em cibersegurança se relacionam com os requisitos de conformidade, que forçam as organizações a se concentrarem em controles de segurança e vulnerabilidades. A gestão de riscos considera várias facetas, incluindo ativos, ameaças, vulnerabilidades e controles. Uma organização de cibersegurança integrada funcionalmente coloca as ameaças na vanguarda de práticas estratégicas, táticas e operacionais.

Com todas as novas aplicações inovadoras da Internet, há oportunidades para desenvolver novos produtos e serviços com novas definições de qualidade que se afastam do foco utilitarista convencional e se tornaram um fator de mudança de ambiente e sistemas competitivos [6]. A segurança da Internet e, em geral, da segurança cibernética é agora uma questão de qualidade e requer novas ferramentas e métodos de garantia de qualidade. Este artigo introduz os modos de falha e a análise de efeitos (FMEA) como uma abordagem de qualidade e confiabilidade (FMEA) para avaliar, monitorar e mitigar ameaças à segurança cibernética.

O FMEA é um método de análise de confiabilidade destinado a identificar falhas que afetam o funcionamento de um sistema e permitir que as prioridades de ação sejam definidas. A FMEA foi usada pela primeira vez na indústria de defesa na década de 1940 para produtos militares e é formalizada nessa indústria nas Normas Militares mil-std-1629A do Departamento de Defesa. Na década de 1950, paralelamente ao trabalho de Juran e Feignbaun, o Departamento de Defesa dos EUA formou um grupo ad hoc sobre confiabilidade de equipamentos eletrônicos. Este grupo se esforçou para prever a taxa de falha do equipamento. O grupo percebeu que a previsão não era suficiente e desenvolveu uma abordagem da FMEA para reduzir as taxas de falha ao longo do tempo [7].

A FMEA é um grupo sistemático de atividades destinadas a (a) reconhecer e avaliar a potencial falha de um produto ou processo e os efeitos dessa falha, (b) identificar ações que possam eliminar ou reduzir a chance de potencial falha ocorrer, e (c) documentar todo o processo. O resto do jornal é organizado da seguinte forma. A seção "Revisão de Literatura" apresenta uma revisão da literatura relevante sobre a FMEA e suas aplicações, suas vantagens como abordagem à segurança cibernética e sua eficácia, e uma breve discussão sobre o uso da FMEA para avaliar ameaças e riscos dos sistemas de informação como ferramenta de segurança. Na seção "Utilização da FMEA para avaliação de riscos e cibersegurança", os autores apresentam a base teórica e o desenvolvimento do modelo com uma discussão sobre segurança da informação e como a confidencialidade, integridade e disponibilidade podem ser vistas como questões de qualidade, juntamente com a metodologia proposta e etapas específicas para a implementação da FMEA para a segurança cibernética. Um exemplo hipotético de um aeroporto é apresentado para demonstrar a implementação da FMEA para mitigar o risco de ameaças à segurança cibernética. Finalmente, as conclusões oferecem um roteiro para outras organizações que desejam implementar a FMEA para melhor proteger seus sistemas de informação e questões relacionadas.

CONCLUSÃO

Este artigo oferece uma abordagem única para gerenciar a segurança dos sistemas de informação. A metodologia C-FMEA proposta tem várias vantagens em relação às abordagens tradicionais de gestão de riscos. O principal impulso do papel é considerar a segurança como uma questão de qualidade, (ou seja, um sistema de informação de alta qualidade é aquele que processa, comunica e produz dados com alto nível de confidencialidade, integridade e disponibilidade). A metodologia proposta incorpora essas três dimensões da segurança de TI na abordagem tradicional da FMEA já utilizada na fabricação ou sistemas de serviços. O processo de proteção das redes organizacionais e seus sistemas de informação é um processo contínuo, e os autores propõem o processo C-FMEA como um projeto contínuo. Os administradores e consultores do

sistema podem usar a abordagem para analisar qualquer vulnerabilidade em um sistema de informações existente e oferecer recomendações proativas para proteger o sistema contra possíveis ameaças.

O C-FMEA proposto é uma ferramenta qualitativa e sistemática, tipicamente criada dentro de uma planilha, para ajudar os praticantes a antecipar que as coisas podem dar errado com um sistema de informação em geral ou seus componentes. Além de determinar como um sistema de informação pode falhar, a C-FMEA também ajuda a encontrar as possíveis causas de falhas e a probabilidade de falhas antes de sua ocorrência. A capacidade de antecipar problemas de segurança precocemente permite que os administradores de cibersegurança evitem possíveis falhas ou vulnerabilidades. Os autores demonstraram a metodologia proposta utilizando um exemplo hipotético. Trata-se de um exercício de aprendizagem, e os autores pretendem implementar a metodologia em um ambiente real de caso.