Journal of Computer Networks, 2024, Vol. 12, No. 1, 1-6
Available online at http://pubs.sciepub.com/jcn/12/1/1
Published by Science and Education Publishing
DOI:10.12691/jcn-12-1-1

Cybersecurity Data Sources and Practices

Cheryl Ann Alexander[1,*], Lidong Wang[2]

[1]Institute for IT Innovation and Smart Health, Mississippi, USA
[2]Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA
*Corresponding author: cheryl.alexander@techhealthsolutions.org

Received July 04, 2024; Revised August 05, 2024; Accepted August 12, 2024

Abstract Today, with technology exploding in every organization, massive amounts of data are being generated, thus, approaches to processing such huge amounts of data are necessary and key to threat detection and cybersecurity. Currently, artificial intelligence (AI)/machine learning (ML), and cyber automation help to process these huge amounts of data, however, much of the data is unstructured and unlabeled and can be a considerable challenge for off-the-shelf AI/ML. This paper introduces cybersecurity data sources; the functions, features, limitations, and future trends of security information and event management (SIEM); potential enhancements of future SIEM; offense data and defense data; and data sources and AI for SIEM. Cybersecurity data sources and practices are also discussed in a large medical center as a case study. Data sources in healthcare can be internal or external. Offensive and defensive strategies must include where the data comes from and how the data is used. A future enhancement of SIEM is beneficial such as improving prediction, detection, correlation, and reaction capabilities. Networks are the platform of cyber data sources and practices (such as data storage and transfer), networked medical equipment, health monitoring, SIEM, and even malicious attacks. A key to robust cybersecurity is to enhance the security of computer networks.

Keywords: *cybersecurity, network, offense data, defense data, Internet of things (IoT), Internet of medical things (IoMT), artificial intelligence (AI), machine learning (ML), healthcare*

Cite This Article: Cheryl Ann Alexander, and Lidong Wang, "Cybersecurity Data Sources and Practices." *Journal of Computer Networks*, vol. 12, no. 1 (2024): 1-6. doi: 10.12691/jcn-12-1-1.

1. Introduction

AI/ML and cyber automation can process huge data from various sources, vital to threat detection and cybersecurity. Cybersecurity data can be internal or external. Security information and event management (SIEM) systems focus on data sources internal to an enterprise. There are limitations in the current SIEM. The National Institute of Information Systems and Technology (NIST) emphasizes anomaly detection in real-time, intelligent visualization, quick responses, and effective management of incidents, etc. [1,2].

Much of the data in the cybersecurity area is unstructured and unlabeled. This is a challenge for users to use off-the-shelf AI/ML methods. It introduced how cybersecurity data is inherently relational/graph-structured and how graph-based ML (graph ML) can achieve improved unsupervised results. The graph structure helps make up for the lack of labeled data. Many security relationships fit well into graph learning. Graph ML can provide useful visualization of model outputs. This is better than the displayed tables of traditional ML results that are not as interpretable and intuitive as the graph display. Graph ML will make a great impact on the next-generation cybersecurity systems [3].

Cyber threat intelligence (CTI) is an integral of cybersecurity capabilities in an enterprise. It is often a challenge to extract actionable CTI. The challenge is related to CTI data sources (capture, storage, processing, visualization, etc.) and accessing and choosing relevant CTI data sources [4]. CTI is an adaptive technology that can leverage a huge amount of threat history data and can proactively block and mitigate future malicious attacks on a network.

Since medical procedures, diagnostics, and health data have been becoming electronic, cloud-based, and distributed among many stakeholders, healthcare systems have been targets of malicious third parties. The features that make SIEM solutions essential in healthcare are 1) real-time analytics, 2) self-learning configuration management database, 3) scalable log management, 4) multi-tenant management, and 5) compliance reports. SIEM provides a united and global look into enterprise's security events, which helps keep health data safe and prevent HIPAA (Health Insurance Portability and Accountability Act) violations [1,5,6].

The purpose of this paper is to introduce cybersecurity data sources; the functions, features, limitations, and future trends of SIEM; potential enhancements of future SIEM; offense data and defense data; and data sources and AI for SIEM. Also, cybersecurity data sources and practices are discussed in a large medical center as a case study. Data sources in the medical center can be internal or external. Offensive and defensive strategies must

include where the data comes from and how the data is used. Accountability for data source strategies should be a joint effort between management and the IT team.

2. SIEM and Cybersecurity Practices

SIEM systems have been used to prevent, detect, and react against cyberattacks. SIEMs are an important part of any enterprise's cybersecurity ecosystem or environment. SIEMs give IT security teams a central area where collecting and aggregate data so that massive volumes of the data can be analyzed. SIEMs effectively streamline security data sources. Table 1, Table 2, Table 3, and Table 4 show the functions, features, limitations, future, and potential enhancements of SIEMs [1,7,8,9].

Guaranteeing a person's privacy has become stricter with the implementation of the General Data Protection Regulation (GDPR). There are new challenges for the implementation of SIEMs due to GDPR. Table 5 [10,11] shows technical measures and requirements that are needed for the implementation of a SIEM to ensure compliance with GDPR.

Table 1. Functions or features of SIEMs

Functions or Features	Descriptions
Correlation rules	Most SIEMs have basic correlation rules.
Real time processing	SIEMs need to analyze huge events/incidents in real time.
Data analytics	Analysis (e.g., using ML) of the behaviors of employees, third-party contractors, and other collaborators of an enterprise for detecting misbehaviors.
Security	Evaluating the ability to perform security automation and native encryption capabilities in an SIEM.
Storage	Evaluating the length at which an SIEM keeps data stored for further processing or forensics operations.
Reaction and reporting	Reacting against security incidents (including sharing and reporting).
Data sources	Most SIEMs support various types of data sources natively.
Data volume	Large volumes of data from different sources.
Risk analysis	Risk analysis on the assets of the managed infrastructure.
Scalability	Considering the ability for a SIEM use to grow in terms of not only hardware but also the number of security events collected.
Resilience	Considering what the fault tolerance capabilities of an SIEM are.
Complexity	SIEMs are known for being difficult to use and manage. It is important to know if a system can be installed for testing with low or moderate effort.
UEBA	Evaluating if an SIEM has native User and Entity Behavior Analytics (UEBA) capability, or if it provides integration with third-party UEBA solutions.
Visualization	Lack of proper data visualization and little support for interactive exploration of data hinder the analysis of events. Data visualization and custom dashboards are important.
Forensics	Some SIEMs offer built-in network forensic capabilities.
Price	Most SIEMs are expensive according to the evaluation of the licensing method associated with the SIEMs and the limits in the number of users, alerts, correlations, dashboards, etc.
Performance evaluation	Evaluating the performances of SIEMs according to their data storage capabilities, computational capacity, rule correlation processing, as well as data index, search, and monitoring.

Table 2. Limitations of current SIEMs

Limitations	Descriptions
Limited data visualization	Although SIEMs offer data visualization, most of the visual representations are generic, not designed with particular
Reliance on humans	Threat responses sometimes require humans to perform analysis and make decisions, which is slow, costly, and error-prone and requires a high level of expertise.
Incomplete data	Few SIEMs correlate DNS traffic, end-point data logs, and email logs. By law, a person's identity and privacy cannot be disclosed. Correlation does not work well without all data of users and high value assets.
Basic storage capabilities	Usually storing raw events for a limited amount of time to limit the storage space, which may be insufficient for certain incidents.
Basic correlation rules	Current SIEM correlation rules are weak. Few SIEMs have a built-in advanced correlation engine.
Basic reaction and reporting capabilities	SIEMs support reporting alarms. However, most of the systems do not provide pre-configured and customized actions to be triggered.

Table 3. Future of SIEMs (focusing on technological factors)

Technologies	Descriptions
Mobile technologies	A trend of using company-owned devices and personal devices for office work.
ML	Making event detection and decision-making smarter.
5G networks	Increasing the data transfer speed and affecting the amount of data analyzed by an SIEM.
Cloud storage	More efficient in storage and Big Data analytics.
Cloud service integration	More focused on executing software in a remote server, possibly ensuring scalability and high availability of software applications.
Social media analytics	Providing much information and analytics.
Big data analytics	Powerful in the real-time analysis of events.
Internet of Everything	Capturing, managing, and leveraging huge data; extending the IoT by also including people, processes, locations, etc.

Table 4. Potential enhancements of future SIEMs

Potential Enhancements	Descriptions
Enhanced storage	Developing a SIEM extension that handles data archiving in a reliable, flexible, and secure manner leveraging public clouds.
Diverse security	Enhancing SIEMS with diversity-related technologies (e.g., ML) and diverse inputs.
Integration with SOAR	Integrating evolved and adaptive SOAR (Security Orchestration Automation and Response) solutions with dynamic interaction capability.
OSINT data fusion	Providing more comprehensive data on threats using sources of open source intelligence (OSINT).
AI/ML capabilities	Improving prediction, detection, correlation, and reaction capabilities.
Enhanced visualization	A rich set of specialized visualization models for diverse types of data. Effective overviews, interactive capabilities to focus on details, and mechanisms to compare individual and/or groups of data instances. Visualization models with the capability of handling dynamic data to support real-time analysis and decision-making. A visual summary of user activities that reveals common/abnormal patterns.
Other potential enhancements	Development of risk-based metrics; allowing to score the risk for the different operational and functional areas; extending attack propagation and impact metrics. Moving towards a hierarchy of SIEMs and creating collaborative mechanisms due to IoT, 5G, and thus affected SIEM architectures. Integration of SIEMs with extended detection and response platforms. Providing more autonomy and less effort in its utilization and management.

Table 5. Technical measures and requirements

Technical Measures & Requirements	Description
Restrict access to personal data	The restriction is necessary.
Guarantee personal data security	Suitable security measures for the risks of personal data.
Audit and monitor access to personal data	Operations acted by users on personal data.
Notify of any data breach	Utilizing alerts for data breaches.
Permit retention times for personal data	Permit to define various retention times considering data categories.
Permit the pseudonymization of personal data	Replacing personal data with artificial identifiers stops the identification of the holder; this process is reversible.
Permit anonymization of personal data	Replacing personal data with artificial identifiers stops the identification of the holder; this process is not reversible.
Guarantee protection by design and by default	Designing security measures during the development of products, guaranteeing that only required personal data are used and processed.
Guarantee disaster recovery	Guaranteeing disaster recovery planning solutions.
Guarantee resilience	Guaranteeing fault tolerance or resilience.
Be able to create compliance reports	Creating reports with the information required for various compliance regulations.

3. Offense Data and Defense Data

Most cybersecurity research focuses on defensive approaches to preventing the occurrence of vulnerability. Proactive approaches are also needed due to old, emerging, and unknown cyberattacks; therefore, many offensive security exercises such as penetration testing and adversary simulation have been conducted. A hybrid model was developed for launching offensive security exercises to capture, determine, and understand attack patterns. This method is used to uncover tactics, techniques, and procedures through threat hunting via adversary emulation. It helps detect unknown threats [12].

Data defense is about minimizing downside risk. Data offense focuses on supporting business objectives such as increasing revenue, profitability, and customer satisfaction. Table 6 [13] shows the comparison of offensive data strategy and defensive data strategy. Striking the best balance between offense and defense is a challenge but an important issue. Information operations (IOs) need the coordinated understanding of targets existing in physical, symbolic information, and cognitive domains. The conduct of defensive and offensive IOs needs coordinated targeting and protection, respectively, across the three domains. Data fusion was studied to provide intelligence for IOs and perform both defensive and offensive IOs [14].

Table 6. Offense data versus defense data

Aspects	Offense	Defense
Data management	Flexibility	Control
Key objective	Improve competitive profitability and position	Guarantee data quality, integrity, privacy, security, regulatory compliance, and governance
Core activities	Optimize data modeling, transformation, analysis, visualization, and enrichment	Optimize data extraction, standardization, storage, and access
Enabling architecture	Multiple versions of truth (MVOTs)	Single source of truth (SSOT)

4. Data Sources and AI for Cybersecurity

AI-based SIEMs are often good at utilizing ML algorithms to analyze historical data, detect patterns in the data, and calculate potential threats. It is key that the use of predictive analysis is particularly useful when the IT team wants to identify potential threats before occurrence. This can enable enterprises to take proactive measures to

prevent cybersecurity attacks. Some cybersecurity data sources and their descriptions are shown in Table 7 [15]. Table 8 summarizes important themes of AI for cybersecurity within large communities: security operation centers (SOCs), CTI, adversarial ML, and disinformation and computational propaganda [15].

Table 7. Some data sources of cybersecurity

Types	Data Sources	Descriptions
External	Conventional social media	Sites that facilitate social networking, e.g., YouTube, Facebook, Twitter
	Internet-Relay-Chat	Plain-text instant messaging chatrooms (often used by hacktivist groups)
	News sources	Public media sources (sharing news)
	Paste sites	Sites that permit the anonymous posting of plain-text contents
	Social coding repositories	Sites that enable the sharing of code in repositories
	Hacker forums	Online discussion boards that permit hackers' discussion of malicious attacks
	Carding shops	Sites that sell stolen credit cards
	Malware repositories	Sites that aggregate malware and report
	Search engines of IoT	Engines that search and index publicly accessible IoT devices
	DarkNet marketplaces	Markets that facilitate the sale of illicit goods
	Commercial threat feeds	Feeds of threat intelligence data curated by industry
Internal	Data storage	Devices that store data from networks and users
	Intranets and social media, and reports	Tools to facilitate collaborations across teams
	Networking devices	Devices that help route and facilitate network traffic
	Netflow data	Flow of data across networked devices
	Workstations and/or virtual machine images	Machines that enable and facilitate computational activities
	Network-based fingerprint data	Data that pertains to the content generated from a device
	Vulnerability assessment	Reports generated from vulnerability scanning tools
	Alert and event logs	Succinct reports and short alerts about selected network and/or device events
	Biometric data	Data generated from sensors that monitor human behaviors

Table 8. Some cybersecurity application areas of AI

Application Areas	Examples of Common Tasks
SOCs	Intrusion detection, vulnerability evaluation, analysis of log files
CTI	Phishing detection, malware analysis, Dark Web analytics
Adversarial ML	ML poisoning, malware evasion
Disinformation & computational propaganda	Disinformation identification, Bot detection

5. Data Sources and Cybersecurity in a Large Medical Center

5.1. Defense Data Strategy and Offensive Data Strategy

Charleston Regional Medical Center in Jackson, Mississippi, USA practices robust cybersecurity for employees and all patient visits. The defense data strategy in the Medical Center lies in protecting patient data and privacy and following the guidelines set in place by HIPAA and other federal laws, etc. Patient data is a critical part of taking care of patients. Patient data is generated by providers, nurses, clinicians, etc. as they take care of their patients and record clinical data. Patient privacy is essential in any hospital setting. Patient privacy is protected by physical methods such as screen protectors, location, passwords, etc., while it is also protected by security methods such as HIPAA, HiTECH, and other federal programs. Other methods of avoiding a data breach include restricting access to patient information and protecting sensitive information with passwords. The reputation of the hospital is sensitive to protecting the data if there are continued breaches of sensitive patient data the hospital's reputation may be affected and patients may not seek care at that facility, particularly if there are continual data breaches.

The offensive data strategy should focus on making the hospital more competitive and keeping services satisfying to the public. Most hospitals have a compliance department that functions to keep data secure and employees functioning within the guidelines set by the federal government and the hospital. Some offensive strategies include project management, surveys from patients that indicate problems with service, and spot checks for each clinical department such as nursing, providers, therapists, etc. Government agencies such as AHRQ (Agency for Healthcare Research and Quality) set certain standards that must be kept up. The Health and Human Services department also sets standards that keep clinical staff operating at a highly focused level of service. This is called a Magnet Level Hospital where staff are highly trained, focused on quality, and focused on patient satisfaction.

Table 9. Some data sources of cybersecurity in the Medical Center

Types	Data Sources	Data Examples
External	Alert systems for tornado, trauma, etc.	Patient information
	Patients/victims of trauma or natural disasters	Health information
Internal	Computers, mobile devices, laptops, or tablets	Medical reports
	Provider mobile devices	Clinical data
	Data center services	Financial information (e.g., billing, insurance), research data, etc.
	Servers and storage devices	Electronic health records (EHR), digital pathology reports, etc.
	Software in the Medical Center	Medical images, clinical notes, etc.
	Medical devices for patient monitoring and diagnosis	Medical images
	Scanners	Biometric data such as fingerprint
Internal or external	Key networked medical equipment (ventilators, IV pumps, etc.)	Clinical data
	IoT and IoMT	Patient signs and diagnosis data

Striking a balance between offensive and defensive strategies is a key issue for the Medical Center. It is

difficult to keep a balance between the two. However, for some hospitals, an optimal balance requires striking a balance between patient satisfaction and the protection of patient data. Sometimes it is necessary to favor one over the other and it depends on the specific situation and availability of resources in the Medical Center and the management level of cybersecurity. Some data sources of cybersecurity in the Medical Center are shown in Table 9.

5.2. External Data Sources

Patients of car accidents, tornadoes, house fires, shootings, etc., may find their patient information compromised as very tight cybersecurity is unlikely during mass casualties, traumas, natural disasters, etc. Patients who are victims of mass casualties or large natural disasters may have their health information exposed or manipulated. This lack of structure when going through a mass casualty or trauma can severely cost the patient.

5.3. Internal Data Sources

Medical reports are clinical notes written by providers, nurses, and ancillary clinical staff on a computer, mobile device, laptop, or tablet. Medical reports become a part of the clinical patient records or electronic health records (EHRs) and contain sensitive diagnostic, treatment, evaluation, and other clinical information about the patient. Provider mobile devices are used by clinical staff to save time and can contain clinical information, and information that providers need to treat the patient such as diagnostic or treatment plans, imaging data, billing data, and other information providers may find useful in treating the patient. Mobile devices may include cell phones and tablets. These devices contain sensitive information about the patient.

Data center services handle financial information, research data, and more for the Medical Center. Financial information includes billing, insurance, etc. This information is highly attractive to malicious actors for its sensitive information and the value of the presented information. Patient insurance information and billing data are far more valuable than social security numbers or general information as malicious actors can sell the patient's insurance information to a third party who may prevent the patient from getting insurance coverage or cause rate hikes.

Traditional healthcare facilities use data storage options vital to protecting electronic medical records (EMRs), EHRs, patient health information (PHI), digital pathology reports, next-generation sequencing results, and other sensitive information. Common methods of data storage include on-premises, cloud, and hybrid measures. Personal information, and patient records (e.g., EMRs, EHRs, or PHI) are poorly protected during mass casualty events as the priority is getting the patient to safety. PHI includes all patient data including stored information, current information, treatment, imaging, diagnostics, etc.

Much software has been used in the Medical Center for access controls, intrusion/attack detection, diagnosis, medical image processing, clinical notes, etc. Medical images are produced by X-ray, doppler, ultrasound, CT, MRI, ECHOs, PET, etc., and are susceptible to cyberattacks. These devices are used in diagnosis and treatment. Scanners such as barcoding scanners and biometric scanners (e.g., fingerprint scanners, face recognition scanners, and iris scanners) have been widely used in hospitals for authentication, access control, patient tracking, medication delivery, etc.

5.4. Internal or External Data Sources

Key networked medical equipment includes ventilators, IV pumps, heart rate monitors, defibrillators, etc. The data sources of the medical equipment are internal when staff produce clinical data and equipment belonging to the medical center; while data sources of the medical equipment are external when equipment belongs to or is inside the patient e.g. defibrillator, heart monitor, etc. This networked equipment must be protected because any alteration in the settings can be potentially fatal. Any malicious actor can access the equipment using the network to implant malware which can cause possibly fatal alterations.

Ventilators provide a breathing response when the patient is unable to. Malicious actors can attack the ventilators by altering the rate of breathing, and the amount of oxygen flowing through the ventilator. Such alterations can cause serious or fatal responses in the patient. Manipulating the settings on the ventilator can be a deadly situation for the patient. IV pumps are another piece of medical equipment that malicious actors can alter and cause serious or even fatal results. When the patient is on a life-saving infusion and the rate of the infusion is altered to be less or more than the provider ordered, the patient can get into serious trouble. Heartrate monitors and defibrillators are also networked and vulnerable to malicious actors. A slight change in the settings may prove fatal. This includes both internal and external equipment.

IoT and IoMT generate huge amounts of data that can be internal (within the Medical Center) or external (for remote telehealth or telemedicine). Various types of data such as patient vital signs, treatment data, notes, orders, and diagnosis data will be generated and processed. Both IoT and IoMT can be attacked by malicious actors, which will affect the functionality of IoT and IoMT and generate bad data. Data generated by IoT and IoMT can also be attacked, which will destroy data security and patient privacy.

6. Conclusion

In today's technological environment, huge amounts of data are generated, therefore, methods to process such huge amounts of data are necessary. AI/ML and cyber automation can process huge amounts of data. Much data is unstructured and unlabeled and can be a significant challenge for off-the-shelf AI/ML. Cybersecurity data sources have been presented and it is essential to note that SIEMs have been used to react, detect, and prevent cyberattacks. However, SIEMs have limitations, for example, limited data visualization and a potential for error-prone and costly limitations. A future enhancement of SIEMs is beneficial such as improving prediction, detection, correlation, and reaction capabilities.

Data sources can be internal and external and strategies

to fight malicious actors depend on various factors, such as the cybersecurity level (e.g., the capability of the IT team) and the management level of an organization, where cyber data sources are located, etc. In a large hospital or medical center, striking a balance between offensive and defensive strategies is necessary and significant. Data sources, defense data strategy, offensive data strategy, and cybersecurity in Charleston Medical Center were presented as a case study. Networks are the platform of cyber data sources and practices (such as data storage and transfer), networked medical equipment, health monitoring, SIEM, and even malicious attacks. A key to robust cybersecurity is to enhance the security of computer networks.

ACKNOWLEDGEMENTS

The authors would like to express thanks to Technology and Healthcare Solutions, USA for its help and support.

Conflict of Interest

The authors would like to announce that there is no conflict of interest.

Ethics

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

References

[1] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759.

[2] National Institute of Standards and Technology. (2015). Guide to industrial control systems (ICS) security- NIST special publication 800-82, revision 2. https:// nvlpubs.nist.gov/ nistpubs/ SpecialPublications/ NIST.SP.800-82r2.pdf.

[3] Bowman, B., & Huang, H. H. (2021). Towards next-generation cybersecurity with graph ai. *ACM SIGOPS Operating Systems Review*, *55*(1), 61-67.

[4] Mtsweni, J., & Mutemwa, M. (2019, July). Technical guidelines for evaluating and selecting data sources for cybersecurity threat intelligence. In *Proceedings of the ECCWS 2019 18th European Conference on Cyber Warfare and Security* (pp. 305-313).

[5] Biddle, S. (2017). Why SIEM solutions are essential to securing healthcare networks. Fortinet Article.

[6] O'Dowd, E. (2016). How SIEM solutions work to secure health IT infrastructure. HIT Infrastructure, Xtelligent Healthcare Media Report.

[7] Hollister, A. (2021). Similarities and differences between XDR and SIEM. Forbes Technology Council Post.

[8] Serckumecka, A., Medeiros, I., Ferreira, B., & Bessani, A. (2019). A cost-effective cloud event archival for SIEMs. In *2019 38th International Symposium on Reliable Distributed Systems Workshops (SRDSW)* (pp. 31-36). IEEE.

[9] Tankard, C. (2019). Goodbye SIEM, Hello SOARX. *Network Security*.

[10] Vazao, A., Santos, L., Oliveira, A., & Rabadao, C. (2021, June). A GDPR compliant siem solution. In *European Conference on Cyber Warfare and Security* (pp. 440-XIV). Academic Conferences International Limited.

[11] Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (GDPR). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, *10*(3152676), 10-5555.

[12] Ajmal, A. B., Shah, M. A., Maple, C., Asghar, M. N., & Islam, S. U. (2021). Offensive security: Towards proactive threat hunting via adversary emulation. *IEEE Access*, *9*, 126023-126033.

[13] DalleMule, L., & Davenport, T. H. (2017). What's your data strategy. *Harvard business review*, *95*(3), 112-121.

[14] Waltz, E. (2000, June). Data fusion in offensive and defensive information operations. In *NSSDF Symposium.*

[15] Samtani, S., Kantarcioglu, M., & Chen, H. (2020). Trailblazing the artificial intelligence for cybersecurity discipline: a multi-disciplinary research roadmap. *ACM Transactions on Management Information Systems (TMIS)*, *11*(4), 1-19.