Automated Risk Analysis Tooling in Cybersecurity

Group 2

Naif Alanazi - Hassan Alshehri

12/4/2023

Automated Risk Analysis Tooling in Cybersecurity

Introduction

Analyzing the cybersecurity risks is critical to the overall strategy of safeguarding an organization’s information systems or digital infrastructure. However, the modern risk management architecture requires a robust integrated plan that regularly assesses risk susceptibilities in internal and external environments and presents the outcomes in simplified forms (Matheu-García et al., 2019). This observation implies that manual processes cannot provide a comprehensive picture of the organization's cybersecurity status, especially in the contemporary big data environment. Against this background, automated risk analysis tools have become almost indispensable to cybersecurity plans. These tools are designed to help the management identify, evaluate, and manage information risk in real-time. They rely on advanced algorithms and models to connect the dots and give the management an overall picture of what is going on, including the mitigation measures required and how they are supposed to be prioritized based on threats' severity (Gonzalez-Granadillo et al., 2021). As such, an organization can make informed decisions on what resources are needed and how they should be utilized.

Today’s business environment is rapidly evolving, suggesting that risk assessment tools must also transform to keep up with these changes. As observed by Ghillani (2022), these tools must be automated by taking advantage of advanced technologies such as artificial intelligence (AI) and machine learning (ML) to improve their effectiveness in evaluating and analyzing potential risks and proposing mitigation strategies. The growing demand for automation emanates from the complexity and amount of data that must be processed to get relevant information, as well as the increased need for efficient risk management processes. This paper investigates the concept of automated risk assessment tooling in cyber security to shed light on how they can be implemented, their features, advantages, challenges/limitations, and the projected future trends. A large health system in Michigan is used as the case study.

It starts by providing the background to the research topic, including describing the relevant security concepts related to automated risk analysis tooling in cybersecurity, whereby the historical work on this issue is reviewed and the company scenario described in details. After that, the method used to achieve the project's objectives is described. In this case, since the project was more analytical than implementation-based, a section describing the method used to avoid biases during the analysis is provided. The final section presents the preliminary results obtained using the methods described in the third section.

Background

Before automated risk management tools emerged, the cybersecurity sector relied on GRC (governance, risk management, and compliance) and legacy systems. While many organizations are still dependent on these outdated tools to safeguard their information systems against cyber-attacks, there has been increased realization that legacy technologies are holding businesses back by weakening their information security programs/strategies (Langer et al., 2016). These traditional approaches are associated with several drawbacks:

- Increased interruptions and operational costs.
- Susceptibility to cybersecurity threats.
- Overreliance on manual work.
- Incompatibility with modern systems.

These drawbacks indicate the need for automated risk analysis tooling for cyber security to help mitigate cybersecurity risks cost-effectively. Against this background, this paper investigates the concept of automated risk assessment tooling in cyber security to shed light on how they can be implemented, their features, advantages, challenges/limitations, and the projected future trends. It also provides substantial insights that can help a company boost its cybersecurity resilience through automated risk analysis tooling.

The organization being analyzed is a large health system in Michigan. Its structure includes information security, risk management, and physical security. The head of these departments reports to the Chief Information Privacy and Security Officer (CPSO). Over the last year, the company had paid out 1.5 million dollars in Health Insurance Portability and Accountability Act (HIPAA) fines and penalties, including corrective actions to refine the third-party access and risk management program. These fines and penalties suggest that the organization lacks a health information privacy and security risk management program that can automatically detect, prevent, or mitigate a cybersecurity threat. The hospital uses the following in-house technology (supported and owned by the hospital):

- Various databases for Finance, HR, IT, and Patient Management using SQL Server 2008-2016.
- Various servers using Windows Server 2003-2012.
- The on-premises version of CA Service Desk Manager R7.0 Software is on the Windows 2012 server.

External technology (Supported, Developed, and Owned by Vendors):

- Epic Electronic Health Record (EHR) Cloud Application.
- Microsoft Office 365.
- Microsoft One Drive.
- CA Identity Manager 14.1.

- Discussions have begun to contract with the Amazon Web Services (AWS) platform to move all physical servers to virtual machines (VMs).
    - The health system will be responsible for the privacy and security of the Platform as a Service (PaaS) implementation.
- The health system will acquire dialysis centers and machines from third-party relationships.
- Health Information Exchange agreement with Tri-State Health System, states of Michigan,
- Illinois, and Ohio
- Interdepartmental access agreements to share state-required health information through electronic data interchange (EDI)
    - Public health
    - Mental health
    - Immunology (HIV/AIDs, state reportable sexually transmitted infections)
    - Cancer
- Business associates and vendors (25), 12 with no BAA (business associate agreement) or contract (hand-shake agreement).
    - Transcription service.
    - Medical records.
    - Medical supplies and equipment (vendor).

This analysis shows that the organization depends heavily on external technology (supported, developed, and owned by vendors), with in-house technology being minimal. As such, the findings presented in this paper will open the eyes of the management to the need to have in-house automated risk analysis tools to mitigate cybersecurity risks cost-effectively and avoid losses through fines.

Method

To achieve the study's objectives, a combination of primary and secondary data sources was used. Primary data collection relied on interviews, whereby cybersecurity experts and managers of companies that have implemented security risk management systems in their organizations were interviewed to gain a better understanding of the problem. The potential interviewees were contacted through emails, phone calls, or other online means, such as social media platforms. The purpose of contacting them was to seek consent and arrange the interview, whereby the research purpose, means of ensuring confidentiality, and the length and format of the interview were explained.

Open-ended questions were asked to facilitate discussions. Some of the questions asked included whether they have automated their risk analysis tools or are still dependent on legacy programs. Those who have not automated were asked the reasons, while those who have automated will be asked to share their experiences and challenges. The responses given helped in assessing the advantages and challenges/limitations of automating risk analysis tools. Conducting the interviews was also critical in this study because it brought new insights concerning how automated risk analysis tools are implemented and the anticipated future trends. A thematic analysis approach was used to analyze the participants' responses, whereby themes related to the topic were identified.

Secondary data collection involved a review of available literature regarding the topic to understand the problem's background, as well as the meaning and implications of automated risk analysis tooling. Online databases, such as Google Scholar, were used to retrieve credible and up-to-date sources concerning the subject topic. The criteria for selecting these sources included credibility, currency (publication date), objectivity, and authority. To ensure that the information obtained from these sources is credible and objective, most of the sources retrieved are peer-reviewed articles. Credible websites were also used to get relevant information that can help in developing arguments. They included government and university websites.

Results

As indicated in the introduction, this paper aimed to shed light on the implementation, features, advantages, challenges/limitations, and the projected future trends of automated risk analysis tooling in cybersecurity. The primary themes emerging from the included the assertion that securing systems and networks has become a significant concern for many organizations, thus increasing the demand for innovative solutions that can automatically detect risks and take the necessary measures to prevent or mitigate them. Some of the features highlighted regarding these tools are that they are designed to scan for susceptibilities in computer systems and networks and monitor any abnormal occurrences that could lead to violations of systems' integrity. In other work, they seek to determine the cybersecurity status of the assessed entity and provide relevant information regarding potential risks, threat impacts, and associated costs. Nonetheless, like any other innovation, the interviewees indicated that automated risk analysis tools have upsides and downsides that should be considered before implementing them.

The upsides/advantages of having an automated risk analysis tool include minimizing human errors and biases, improving accuracy and efficiency, cost-effectiveness, and facilitating informed decision-making. This finding is consistent with Matheu-García et al.'s (2019) finding that automated risk analysis tools can provide significant benefits to an organization, including real-time risk monitoring, improved decision-making, and mitigating human errors and biases. It implies that when a company or an individual has an automated risk analysis tool, their systems are monitored in real-time, allowing swift scanning and monitoring of susceptibilities in a system. The improved accuracy and efficiency are attributed to the fact that most manual work is replaced by a tool, thus minimizing most of the errors associated with human mistakes. It is also worth noting that when the assessment of cybersecurity risks is automated, the need to outsource services or hire many employees to carry out such a task is minimized, thus reducing operational costs. This view was shared by most interviewees, who suggested that the reduced number of employees and improved efficiency are among the factors that make automated risk analysis tools cost-effective. Regarding improved decision-making, it emerged that the ability of these tools to monitor risks in real time provides decision-makers with valuable information they can use to make informed decisions rather than relying on intuition.

Despite these benefits, several drawbacks were identified, including the possibility of these tools giving false positives, thus misinforming the decision-makers and directing their attention to non-existent risks. Another theme emerging from the interviews is that automated risk analysis tools lack the flexibility associated with a human being, thus giving limited insights. This inflexibility also makes the tools less proactive, especially in addressing evolving threats. The other downside of these tools is that they require regular updates to equip them with the ability to deal with emerging threats.

Future Work

The findings presented in this paper provide the foundation from which future studies can be conducted. For instance, future studies can focus on finding solutions to the several drawbacks associated with automated risk analysis tools in cybersecurity. In particular, they can examine how these tools can be made more proactive and flexible to deal with emerging threats, considering that the environment in which modern businesses are operating is evolving constantly. As observed by Ghillani (2022), today's businesses are operating in an environment characterized by complex and voluminous data that must be processed to get relevant information. These challenges require responsive and efficient risk management tools and processes. Future researchers should also examine the potential of advanced technologies such as artificial intelligence (AI) and machine learning (ML) to improve the effectiveness and proactivity of existing tools. The recommendations given by interviewees in this study suggested that these technologies could improve risk assessment in organizations. To this end, there is a need for a comprehensive study to investigate the veracity of those claims.

Conclusion

This paper investigated the concept of automated risk assessment tooling in cyber security to shed light on how they can be implemented, their advantages, challenges/limitations, and the projected future trends. It has been established that the demand for innovative solutions that can automatically detect risks and take the necessary measures to prevent or mitigate them has increased considerably in the recent past due to heightened concerns about the evolving threats to information systems and networks. However, like any other innovation or technology, the use of automated risk analysis tools in cybersecurity has both upsides and downsides. The upsides include minimizing human errors and biases, improving accuracy and efficiency, cost-effectiveness, and facilitating informed decision-making. Downsides include false positives, inflexibility, and the need for frequent updates. These drawbacks provide the basis for future studies to investigate the various ways in which the effectiveness of these tools can be improved. Advanced technologies such as AI and ML hold the potential to revolutionize the cybersecurity sector, suggesting the need for future studies to explore how these technologies can improve the existing tools and the anticipated challenges.

References

Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. *Authorea Preprints*.

Gonzalez-Granadillo, G., Menesidou, S. A., Papamartzivanos, D., Romeu, R., Navarro-Llobet, D., Okoh, C., ... & Panaousis, E. (2021). Automated cyber and privacy risk management toolkit. *Sensors*, *21*(16), 5493.

Langer, L., Skopik, F., Smith, P., & Kammerstetter, M. (2016). From old to new: Assessing cybersecurity risks for an evolving smart grid. *Computers & Security*, *62*, 165-176.

Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Computer Standards & Interfaces*, *62*, 64-83.