Modelling the 2021 Microsoft Exchange Server Data Breach in ArchiMate

ARDA KONÇA, University of Twente, The Netherlands

ABSTRACT

In the field of enterprise architecture, enterprise architects and risk and security analysts use various modelling applications to demonstrate how the business goals of an organization are aligned with the overall business systems. In this context, one of the most-used modelling languages is ArchiMate, which allows its users to represent the risk and security-related aspects given that it contains an overlay called "Risk and Security" (RSO). However, despite the guidance of the overlay for its users, it has been noted and highlighted by multiple researchers in the field that it generally lacks clarity and expressiveness when it comes to conceptual modelling of risk and security-related notions. To minimize the drawbacks, and to make the conceptual risk and security modelling as efficient as possible, the researchers in the enterprise architecture field proposed redesigning the mentioned overlay by following a thorough ontological analysis. Yet, their redesign conceptual modelling ideas have not been tested. Therefore, to test out the efficiency, contribution and validity of their examinations and conceptual redesign proposals of the overlay, this research paper models the incident of Microsoft Exchange Server Data Breach 2021 to observe how architects and analysts could express architectural risk and security-related matters more clearly and comprehensively by applying the redesigned concepts of the RSO. Furthermore, this research paper compares this model with another established model describing a different incident based on the original version of the RSO to detect the main differences between both original and redesigned versions.

Additional Key Words and Phrases: Enterprise architecture, ArchiMate, Risk and Security Overlay (RSO), risk modelling, security modelling, 2021 Microsoft exchange server data breach

1 INTRODUCTION

The Enterprise Architecture is a strategic framework that is used by enterprise architects to systematically observe, understand, plan, organize and represent the implementations of business processes, information systems and technology infrastructure. The framework could be considered as a blueprint that allows architects to analyse the complexities of business environments to guide the organizations by assessing gaps and redundancies related to environmental factors which results in achieving better decision-making, more efficient use of resources and a holistic view of the overall enterprise. By modelling such enterprise architectures, the organizations could easily identify, demonstrate and evaluate strategic planning, business objectives, and architectural changes to verify how the overall system aligns with the organization's business goals. This leads organizations to achieve improved decision-making, more effective use of resources, and demonstration of their current business, application and technology components within their enterprise.

In addition to the mentioned achievements, there is an achievement that most of the enterprise architecture frameworks offer: the ability to model risk and security elements within a given context of an enterprise architecture. Given the nature of the business organizations, risky scenarios often have negative impacts on the goals or objectives of a business. To evaluate, mitigate and visualize such risk and security assessments, enterprise architects and risk and security analysts use predetermined elements in their models. For instance, one of the most widely used modelling languages that captures such risk and security-related elements is called ArchiMate. This language suitably covers risk management and incident recovery scenarios by making use of many predefined ArchiMate elements to involve risk and security measures via an overlay called "Risk and Security" (RSO). This overlay is an extension that guides enterprise architects to represent how risk and security-related elements could be visualized within enterprise architecture models.

Although the overlay is a guidance that comes with its notations to define and represent risk and security concepts, it has been evaluated in the paper [4] that the way the concepts are introduced and described in the technical report [1] which is the main original guideline of the overlay, is not quite efficiently expressive, complete and comprehensive in terms of covering all the possible risk and security elements which could occur given a context of a model. For that reason, it has been underlined that the original version of the overlay [1] generally lacks clarity, has redundant intentions and ontological inaccuracies concerning the conceptualization of elements. The referred findings have been found in the research articles [3], [4], [9], [10]. To overcome these problems, the research papers [6], [9] accordingly have proposed a redesigned well-founded RSO version of ArchiMate by suggesting considerable risk and security representation ideas to extend the overlay capabilities and for the enterprise architecture models to become better tools that contain more comprehensive, expressive and detailed display of risk and security elements. To point out, examine, and verify the brought-up gaps, this research paper first studies an established model based on the guidelines of the original RSO version [1]. Then, it applies the well-founded redesigned RSO of the papers [6], [9] to represent a real-world scenario, the security incident of the 2021 Microsoft Exchange Server data breach. Finally, it compares these models to derive some conclusions.

2 PROBLEM STATEMENT

As previously stated, the original RSO [1] has been explored and found to have some conceptual semantic expressiveness, precision and completeness limitations of its notations. However, although there occurred conducted research and approaches to redesign the RSO [6], [9], the researchers' methodology and approaches have not yet been applied to any real-world case on an enterprise architecture model to verify and observe how well the authors' redesign concepts cover the limitations of the original RSO [1]. Because of this gap, this report aims to apply the authors' RSO redesign approaches by modelling a real-world security incident in ArchiMate to validate how well-founded their redesign concepts are.

TScIT 41, July 5, 2024, Enschede, The Netherlands

2.1 Research Question

Due to the semantic restrictions and conceptual completeness drawbacks of ArchiMate's RSO, the problem statement leads to the following main research question of this research paper:

How effective and useful are the redesigned concepts of ArchiMate's RSO proposals mentioned in [6] and [9] have the capability of representing a real-world scenario more accurately and completely compared to the original ArchiMate's RSO [1] guidelines when it comes to model risk and security-related aspects?

This research question can be answered with the following subquestions:

(1) How well do the redesigned concepts of ArchiMate's RSO proposals address the limitations of original approaches in modelling security and risk-related aspects?
(2) How well do the redesigned concepts of ArchiMate's RSO proposals accommodate dynamic and temporal changes and evolving threats in real-world scenarios?

3 BACKGROUND INFORMATION

After carefully analyzing the main research question and its subquestions, it is decided that the subsections under this section should cover the following background contents to be able to answer the main research question: studying the primary risk and security modelling concepts present in the original RSO [1], examining the found identified limitations of both risk and security modelling concepts, and evaluating how researchers have redesigned these concepts to overcome the limitations.

To provide the information, in the first following subsection, there is a table depicted to inform readers what risk and security modelling elements exist in the original version of RSO [1]. Following that, there will be two further subsections dedicated to the purpose of giving details about the researched risk and security modelling limitations to cover the proposed redesigned concepts. These subsections will allow readers to inform themselves about the researchers' perspectives regarding limitations and guide them in understanding how the researchers' redesigned concept ideas address the mentioned limitations.

3.1 Table of Summary of the Risk and Security Modelling Elements in ArchiMate's Original RSO

The elements used in ArchiMate's original RSO [1] to represent risk and security-related concepts are listed in Table **1**. It could be pointed out that with these elements, enterprise architects and risk and security analysts can visualize risk elements to a moderate extent and propose security concepts to produce mitigation plans against those risks. However, the extent necessarily needs to be improved by checking the following studied limitations of the original version of the RSO [1].

RSO Element	**ArchiMate Element**
Threat Agent	Active Structure Element
Threat Event	Business Event
Loss Event	Business Event
Vulnerability	Assessment
Risk	Assessment
Asset at Risk	Resource, Core Element
Control Objective	Goal
Security Requirement	Requirement
Security Principle	Principle
Control Measure	Requirement
Implemented Control Measure	Core Element

Table 1. Summary of risk and security modelling concepts in ArchiMate's RSO by [6]

3.2 Limitations and Redesign Concept Details of Risk Modelling in ArchiMate's RSO

In the research paper [9], the original version [1] of ArchiMate RSO's risk-related notational definitions and their application to enterprise architectures have been extensively analysed and redesigned by researchers in the field. In their research, the researchers follow the concepts of the Common Ontology of Value and Risk (COVER) [10] which is grounded in theories of values, risks, and their interconnections. After establishing these theoretical foundations, their research identified eight limitations considering the risk-related elements. In which, seven of these limitations will be addressed in the incident model, which is as follows:

(1) The original ArchiMate's RSO [1] suggests that the concept of Vulnerabilities related to Threat Events could be modelled as Assessment elements. However, the researchers propose that Vulnerabilities related to an enterprise architectural scenario should be modelled as ArchiMate Capability elements. The authors reason that there is a need to enable the linking of a Capability element to be linked with multiple Assessment elements.
(2) There is no element defined to represent the Capabilities of Threat Agents that pose Threat Events to an organization. To address this limitation, the researchers propose that the Capabilities of Threat Agents could be simply modelled as ArchiMate Capability elements which should be connected to Threat Agent(s).
(3) There is no element defined to represent hazardous situations that activate Vulnerabilities. Therefore, the researchers propose the utilization of a concept named "Hazard Assessment". This concept aims to demonstrate how hazardous situations increase the Likelihood of Threat Events by utilizing ArchiMate Assessment elements.
(4) There is no element defined to represent the Resources that enable Threat Events. To resolve this, the researchers propose to use their introduced "Threat Enabler" ArchiMate Resource element.
(5) There is a lack of relationship between Loss Events and the Goal elements of a Stakeholder. Thereby, the researchers propose connecting a negative influence relationship between the mentioned elements to explicitly make their newly introduced Risk Subject element negatively affected shown in a model.

(6) There is a lack of relationship between the Loss Event and Asset at Risk elements. To overcome this, the researchers propose to connect the mentioned elements with an association relationship to indicate Loss Events are directly associated with Asset at Risk elements.

(7) The researchers think that the main reason why the original version of RSO [1] lacks clarity and expressiveness is that the natural definition of risk is relative, experiential, and polysemic when it comes to modelling the Risk factors. To define and cover the factors to enhance the ability to do risk management more comprehensively, the researchers propose that the risk concepts need to be demonstrated by using three distinct components namely Risk Experience (the "all-connected" grouping of the risk-related elements such as Threat Events, Loss Events, Threat Agents, Threat Enablers, Hazard Assessments, Vulnerabilities and Assets at Risk), Risk (Risk driver element that causes the risk assessment) and lastly the Risk Assessment (the result of risk analysis by taking into account its drivers).

3.3 Limitations and Redesign Concept Details of Security Modelling in ArchiMate's RSO

As for the security modelling limitations of the original version of RSO [1], the research paper [6] has been evaluated. This research paper is based on the concepts of Reference Ontology for Security Engineering (ROSE) [7] to determine the notational limitations related to security modelling in ArchiMate. In this process, six limitations have been identified by the researchers and all the limitations will be addressed in the incident model, which is as follows:

(1) There is redundancy and lack of clarity in representing security elements such as Control Objective, Security Requirement, Control Measure, and Security Principle. To address this gap, the researchers propose connecting the Control Objective and Control Measure elements with a realization relationship. This approach demonstrates and emphasizes how Control Measure elements play a critical role in fulfilling Control Objective elements, without making use of Security Requirement and Security Principle elements.

(2) There is a construct overload when it comes to representing the security element Implemented Control Measure. To address this, the researchers propose to remove the Implemented Control Measure element and introduce a Security Mechanism as a Resource element.

(3) There is a lack of distinction between baseline (as-is version of an enterprise architecture) and target architecture (to-be version of an enterprise architecture) in the means of accounting for changes in the security evolution of an enterprise such as including newly adapted security mechanism(s). To put it differently, according to the researchers, no account of change is represented in the original RSO [1] since the Security Mechanism element was not introduced.

(4) There is a construct deficit in not representing the subjects whose objectives are associated with the introduction of the Security Mechanism element. Because of this reason, the researchers propose utilizing elements, namely the Security Designer (the actor assigned to the implementation of a security mechanism) and Protected Subject (the subject that is a child element of the Risk Subject) respectively.

(5) In the target architecture, it is not possible to represent the conditions associated with the activation of a Security Mechanism. Therefore, it has been proposed to introduce the elements of Security Mechanism, Control Capability, Control Event, and their connected association relationships between each other in the target architecture of a model. Additionally, there is no possible way to visualize how the Control Event elements influence the Control Objective of a Stakeholder and the Likelihood elements that are associated with Threat Events resulting in Loss Events.

(6) There is a lack of missing dependence relationships between the elements such as Threat Capabilities, Vulnerabilities and Goals (intentions of the Threat Agents). To resolve this, the researchers propose making use of association relationships between the specified elements.

4 RELATED WORK

After briefly introducing the elements of what the original version of RSO [1] contains in regards to its risk and security-related modelling concepts from Table **1**, and looking into its revealed limitations and proposed redesign concepts of RSO, this section aims to specifically focus on an additional concept that the researchers came up with in the purpose of enhancing the RSO further.

4.1 Concept of Mutual Activation

The researchers identified an important concept named mutual activation to study and model prevention in their article [2]. This concept serves to model the prevention of threats within a target architecture of an enterprise architecture. To fully acknowledge how enterprise architects and risk and security analysts depict the prevention of threats that trigger further threats, it is recommended to review the following information:

The concept of mutual activation can be described as a generic dependence among the elements Threat Agents, Threat Capabilities, Vulnerabilities, and the motivational Goals associated with the Vulnerabilities.

This concept is underlined in [2], where it is mentioned that the Threat Capability, Vulnerability, and Goal elements are interdependent, forming a mutual activation partnership between them. As a result of this, the researchers highlight that the formed interdependence outcomes enterprise architects and risk and security analysts to identify patterns in the implementation of security mechanisms.

According to the researchers' findings, the analysis to reveal the prevention of threat patterns is mentioned as ontology-driven prevention in security modelling in the literature. To summarize, if any elements that are conceptually mutually activated and an effective security mechanism are present in a model, threat elements that trigger further threat elements can be removed from an enterprise architecture's target architecture. This demonstrates that the activation of the security mechanism leads to the rewarding implementation of preventive measures in security modelling. This prevention concept involves five key threat elements to be removed as a potential threat from the target architecture of an enterprise architecture model.

If the conditions of the mutual activation concept are met, one or more threat elements (depending on the context of an enterprise architecture) that could be removed from the target architecture to reveal the prevention process are as follows:

- Threat Capability
- Threat Agent
- The motivational Goals (intentions) of a Threat Agent
- Vulnerability Capability
- Asset at Risk

4.2 Example Model

After exploring the concept of mutual activation, there is one more related work content that is essential to be referenced as a related work. As mentioned previously, this research purposefully selects an already established model based on the original version of the RSO [1] to compare it to a to-be-created model that follows the redesigned version [6], [9] of the RSO and covers the Microsoft Exchange Server Data Breach incident. The reason for focusing on such an established model is because this research paper not only objectives to employ the redesigned concepts to showcase an incident to see whether the mentioned limitation gaps are reduced and whether the proposed redesigned version [6], [9] of RSO becomes a better guideline for modellers, but it also intends to do comparisons on the concrete models to come up with conclusions of the research. To do so, in this subsection, firstly, the specified chosen model from the paper [9] will be briefly conveyed.

The found-out model that is selected from the paper for comparison sake is about a work-related incident in which an employee gets injured. Below, the model can be spotted.

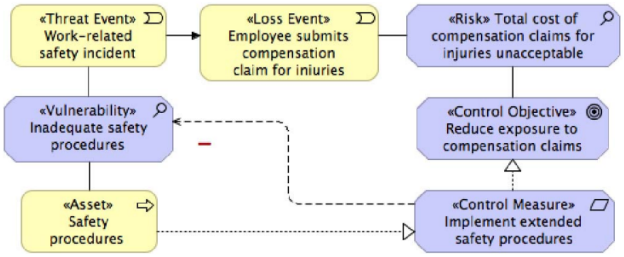
«Threat Event» Work-related safety incident
«Loss Event» Employee submits compensation claim for iniuries
«Risk» Total cost of compensation claims for injuries unacceptable
«Vulnerability» Inadequate safety procedures
−
«Control Objective» Reduce exposure to compensation claims
«Asset» Safety procedures
«Control Measure» Implement extended safety procedures

Fig. 1. Model of the risk of paying compensation claims by [1]

From this model, it could be acknowledged that the Threat Event "Work-related safety incident" triggers the Loss Event "Employee submits compensation claim for injuries" which is associated with the Risk Assessment "Total cost of compensation claims for injuries is unacceptable". In addition to that threat related modelling component, it could be seen that a mitigation plan of the defined Risk Assessment is identified with the implication of the Control Measure. To add more, the Control Measure element is linked to the Vulnerability element by the modellers to communicate that in case the extended security procedures are implemented by an organization, the activation of reducing the vulnerability takes place since there is a negative influence relationship between the elements.

Although one could argue that the drawn risk management and risk plan methodologies of the selected model are sufficiently and simply developed to depict the work-related incident scenario about paying compensation claims from the perspective of an organization, if one gets the motivation to further dig into finding for instance how the Threat Event becomes activated, the only information they would have is the provided Vulnerability, which is not sufficient to take effective steps to do a risk and mitigation analysis of the given model in detail.

After modelling the Microsoft Exchange Server Data Breach incident by following the redesigned concepts, the paper will revisit this model to identify the differences between the two RSO versions by examining the concrete model examples, thereby highlighting the researchers' redesigned concepts' applicability and usefulness.

5 METHODS OF RESEARCH

After reviewing the Related Work Section **4**, it is time to outline the methodology of this research paper. As previously introduced, the goal is to find answers to the main research question of this research paper, which involves modelling the incident of the 2021 Microsoft Exchange Server Data Breach. To achieve this, the author of this research paper did comprehensive literature reviews from multiple sources to gather relevant information on risk and security-related aspects of the incident.

Considering the literature reviews, one of the found useful sources was [8]. This systematic review provides detailed information about the incident which has been studied and thoroughly examined. From the source, it has been learnt that the Microsoft Exchange Server Data Breach incident was not just a simple hack performed by a group of hackers but it was a professional cyber espionage group (named HAFNIUM) backed by a foreign government whose job was to find vulnerabilities in the Microsoft Exchange servers. Their main purpose was to steal email, company data, username and password information from the corporate companies.

5.1 Sequence of Threat Events

The first thing that the group of hackers did to initialize their attacks was that they scanned the Microsoft Exchange Servers on-premises to exploit as much vulnerability as possible. Then, they noticed that the servers were not so secure which consequently led them to perform their attack methods. One of their first attack methods was to send arbitrary HTTPS requests to the servers to gain access by making untrusted connections to server port 443. By doing that, hackers were able to access servers even if they were not a trusted source because of the exploited vulnerability type server-side request forgery (SSRF). After the group of hackers gained access to the servers, they performed remote code executions due to the servers' found deserialization and file-write vulnerabilities. These vulnerabilities allowed the hackers to bypass authentication, write arbitrary files, inject harmful data into the system, and create web shells to maintain access to the compromised servers. After their remote code executions, the group used a tool called 7-zip to compress stolen information from the servers with the intention of data theft. Lastly, the group installed backdoors which they inserted with the motivation of continue maintaining access and use malicious activities against users without being detected by the security protocols of Microsoft even after deployed patches and updates.

5.2 Proposed Defence Solutions

After briefly covering the details of the incident, it is important to discuss the solutions proposed by Microsoft and cloud experts to address the associated risks and threats.

To accomplish this, a systematic review [8] and the following websites [5], [11] were thoroughly investigated to identify the proposed defence solutions. These solutions were used to initiate the modelling of the introduced security mechanism of the incident, allowing for the testing of the redesigned concepts of RSO.

- Patching vulnerable servers to the recommended versions
- Running the Exchange On-Premises Mitigation Tool
- Removing Any Malicious ASPX and ASP.NET Files
- Resetting and Randomizing Local Administrator Passwords
- Investigating Local Users and Groups
- Web Shell Threat Hunting with Azure Sentinel

After reviewing the defence solutions, it is acquired the knowledge that Microsoft did not have a comprehensive approach to analysing security threats, risks, and vulnerabilities related to the Microsoft Exchange Server data breach at the time. It seems Microsoft only released patches after it was too late. Although the previously referred vulnerabilities were reported to them, they were perceived as routine and the overall impact of these vulnerabilities when exploited together was not considered. To avoid such cases, consequently, in the future, it may be beneficial for Microsoft to incorporate enterprise architecture modelling languages such as ArchiMate to better integrate their risk and security management proposals to have their mitigation and prevention plans set up. This could result in performing a more rigorous analysis of their risk and security modelling approach and, if necessary, allow them to propose additional quantifiable countermeasures to mitigate threats and risks.

6 RESULTS

After obtaining sufficient information about the incident, it was time to model it using the proposed risk and security redesign concepts of ArchiMate's RSO. The worked-through model of the incident in ArchiMate is illustrated in Appendix **A** to be examined.

To demonstrate and explain how the redesign concepts of the incident model for the Microsoft Exchange Server Data Breach be aligned and put in an application with the limitations identified in Section **3**, two lists have been compiled: one for redesigned risk modelling and one for redesigned security modelling. These lists specify the particular redesign concepts applied in the incident model to address each previously mentioned limitation of the corresponding subsections **3.2** and **3.3** in order.

6.1 Utilizing the Risk Redesign Concepts on the Data Breach Incident Model

(1) All Vulnerabilities are depicted as ArchiMate Capability elements instead of Assessment elements, each linked to respective Threat Events, as suggested. For instance, the Vulnerability Capability element "Security Evasion" is connected to the Threat Event element "Making Untrusted Connection to Server Port 443," illustrating their relationship. This information provides clear insights into which Vulnerabilities are associated with which Threat Events, aiding risk analysts in their evaluations and implementation ideas of Security Mechanisms.

(2) All Capabilities of the Threat Agent, specifically the "HAFNIUM Hacking Group," are represented as ArchiMate Capability elements. These elements are linked with association relationships to indicate the comprehensive range of capabilities possessed by the Threat Agent, such as creating web shells, performing file write exploitations, and more.

(3) As recommended by the researchers, ArchiMate Assessment elements are used to model "Hazard Assessments," which increase the Likelihood of the occurrence of Threat Events. In the context of the model, this is represented by the Assessment element "Presence of unpatched MS Exchange servers installed on-premises".

(4) To employ the proposed Threat Enabler element, a Resource element labelled "Weak Corporate Security Infrastructure" is identified as the Threat Enabler. In turn, this would give a modeller the idea of how the Threat Enabler turns the sequence of Threat Events into potential Loss Events in the security incident.

(5) To address the limitation of the lack of relationship between Loss Events and the Goal elements of a Stakeholder (Risk Subject), it is determined to connect the Goal element "Corporate Exchange Servers' Data Protection" with the Loss Event "Accessing and Stealing Corporate Emails" by using an influence relationship in the model. This connection allows one to assert that Loss Events negatively influence the Goals of the Stakeholder(s).

(6) To apply the proposed idea of the researchers to this corresponding limitation, it is decided to connect the Loss Events and Asset at Risk elements. Therefore, the Asset at Risk element "Corporate E-mail Data" and the Loss Event element "Accessing and Stealing Corporate Emails" are associated with each other to show which asset is affected by a loss event.

(7) In the baseline architecture of the incident model, while the Risk element is represented by the ArchiMate Driver element "Data Breach of Corporate E-mails," the Risk Assessment is represented by the ArchiMate assessment element "Unacceptable Risk of Compromised Corporate E-mails." Therefore, in the target architecture, the Risk Assessment element is changed to "Acceptable Risk of Compromised Corporate E-mails" to visualize the effectiveness of the implemented Security Mechanisms by not changing the Risk element. This

allows an indication to be included to show how an organization could benefit itself by implementing Implementation Events that are proposed in a Security Mechanism.

6.2 Utilizing the Security Redesign Concepts on the Data Breach Incident Model

(1) To cover the first security modelling limitation, the Control Objective element labelled "Prevention of Corporate Data Breach" and the Control Measure element labelled "Apply Vulnerability Patch Updates" are connected with a realization relationship. In addition, as conveyed by the researchers, the Security Requirement and Security Principle elements are not utilized in the incident model because of their redundancy.

(2) To visualize and illustrate the Security Mechanisms applicable to Microsoft companies using Exchange Servers on-premises, the previously studied proposed defence solutions in subsection **5.2** are modelled within a Work Package as Implementation Events. This demonstrates how the baseline architecture is enhanced by integrating the Work Package to reduce the Likelihood of Threat Events triggering subsequent Threat or Loss Events. This element is labelled as "Introduction of Security Mechanism - Removing the Identified MS Exchange Server Vulnerabilities - Security Update Management". On top of that, the Implemented Control Measure element is not introduced as supported by the researchers.

(3) To apply the suggested redesign concepts for this limitation, the baseline and target architectures are used as ArchiMate Plateau elements to reveal the "as-is" and "to-be" versions of the incident modelling (for the sake of representation of temporal changes), where a Security Mechanism is involved to mitigate the Threat and/or Loss Events.

(4) As stated by the researchers, the Security Designer and Protected Subject are created and labelled as "IT Security Team" and "IT Department" respectively on the incident model, to identify the affected actors whose objectives are associated with the introduction of the Security Mechanism.

(5) The Security Mechanism, Control Capability, and Control Event elements are decided to be used in the target architecture to overcome the corresponding limitation. This usage can be examined where elements are associated together under labels "Security Update Management," "Capacity of Security Patch Updates," and "Applying Released Vulnerability Patches" in sequence. Furthermore, the Control Event "Applying Released Vulnerability Patches" is connected with Likelihood elements to demonstrate its negative influence on the Likelihood of the threat event "Remote Code Execution" triggering another threat event "Using 7-Zip to Compress Stolen Mailbox Data for Extraction and Export," and the sequence of all bundled threat events triggering the determined Loss Event "Accessing and Stealing Corporate Emails."

(6) To overcome this limitation, the association relationships between the elements of Threat Capabilities, Vulnerabilities and Goals are added. This can be seen in for instance where the Goal element labelled "Intention of Stealing Personal and Corporate Data" is linked to the Vulnerability element labelled "Security Evasion" and the Threat Capability element labelled "Sending Arbitrary HTTPS Requests". The relationship between the elements indicates that both Threat Capability elements and Vulnerability elements have a common associated Goal, which gives insights into an organization to how the Goal of a Threat Agent "HAFNIUM" could be planned to be mitigated by risk and security analysts considering its Threat Capability and the organization's associated Vulnerability by following the proposed redesign guidelines.

6.3 Prevention Result Based on the Concept of Mutual Activation on the Data Breach Incident Model

As expressed in the subsection **4.1**, the introduction of the mutual activation concept manifests the possibility of removing threat related elements when the security mechanism is activated under specific conditions from an organization's enterprise architecture model point of view. This methodology is followed in the incident modelling of the Microsoft Exchange Server Data Breach as well, where vulnerability capabilities associated with the Threat Event "Remote Code Execution" were intentionally removed to demonstrate the effectiveness of implementing the security mechanism labelled "Removing Identified MS Exchange Server Vulnerabilities - Security Update Management". This case demonstrates the organization's temporal and future ability to prevent threat related elements [2]. As a consequence, the mutual activation concept introduced by the researchers could be seen as highly beneficial and valuable in addition to applying the redesigned risk and security concepts of RSO.

6.4 Comparison of Two Models

Since the modelling of the incident Microsoft Exchange Server Data Breach as shown under the Appendix **A** is finalized by applying the risk and security redesign concepts, this subsection can now revisit the example model **4.2** to compare both end models to derive conclusions to be able to get insights to answer the main research question.

6.5 Comparison Finding

After comparing both models, the following key finding is derived and highlighted:

The created model of the Microsoft Exchange Server Data Breach incident which follows the redesigned version [6], [9] of the RSO is to a greater extent clearer, complete, and comprehensive in terms of modelling risk and security-related elements compared to the example model from the subsection **4.2** that follows the original version of the RSO [1].

6.6 Reasoning of Finding

The reasoning is that in the example model, it is concluded that there are no elements introduced to represent a Threat Enabler, Threat Capability, Vulnerability Capability, Hazard Assessment, Security Designer, or Protected Subject, due to the nature of the original guidelines of the RSO [1]. Additionally, there is no indication of any introduced Security Mechanism and no possibility to demonstrate how a proposed Security Mechanism could be activated. This is because there are no distinct elements proposed in the original guideline to represent risk treatment components such as Control Event or Control Capability as well as there is no introduced concept of mutual activation.

Given the construct deficiencies and having no threat prevention concept in the original version of the RSO [1], it is inferred that if an organization sticks to the current guidelines, the risk and security analysis processes would be very difficult to manage, thereby complicating the extensive performance of mitigation and prevention planning for identified threats.

Inspecting all these gaps, the redesigned version [6], [9] of the RSO is concluded to provide a clearer, more complete, comprehensive, and expressive conceptualization of risk and security-related matters. This is observed by modelling the Microsoft Exchange Server Data Breach incident by following the redesigned version [6], [9] of RSO and comparing it to a selected model that follows the original version of RSO [1].

7 DISCUSSION

After uncovering and studying the redesigned concepts, data breach incident details, redesigned concepts' application and benefits on the representation of the incident model, and the comparison it is time to answer the main research question and its sub-questions:

7.1 Answer to the Main Research Question

Question: How effective and useful are the redesigned concepts of ArchiMate's RSO proposals mentioned in [6] and [9] have the capability of representing a real-world scenario more accurately and completely compared to the original ArchiMate's RSO [1] guidelines when it comes to model risk and security-related aspects?

Answer: The redesigned version [6], [9] of ArchiMate's RSO is effective, useful and practical in addressing its determined limitations and transforming it into a more correct, precise and complete risk and security guideline by taking into account temporal aspects thanks to the authors' studied concept of mutual activation, their guideline of how to distinctly make use of baseline and target architectures, and their guideline of showing how to introduce and activate Security Mechanism to visualize the prevention of threat elements [2]. These results were obtained after modelling the Microsoft Exchange Server Data Breach incident, so it is possible to deduce that the redesigned version [6], [9] is validly capable of representing a real-world scenario.

7.2 Answer to the First Sub Research Question

The redesigned concepts address the lack of clarity, construct deficiency and construct overload problems in the original ArchiMate's RSO [1], making it a complete and consistent model. The elements such as Threat Capability, Threat Enabler, Security Mechanism, and Control Event have been newly introduced which makes the risk and security modelling efficiently more comprehensive and valid.

7.3 Answer to the Second Sub Research Question

The redesigned concepts of Archimate's RSO distinctly enable the enterprise architects and risk and security analysts to accommodate temporal aspects of risk and security modelling via the use of baseline, target architectures and a work package (implementation of the Security Mechanism). One of the biggest advantages of being able to represent temporal risk and security-related changes is that it is always possible to update target architectures in the presence of new threats and/or threat agents.

8 CONCLUSION

Taking all the conducted research, the application of redesigned concepts, and the answer to the main question into account, the redesigned version [6], [9] of ArchiMate's RSO has proved to be a satisfactorily efficient guideline for applying risk and security construct modelling in real-world scenarios. Based on the applications of the redesigned concepts, it is concluded that any enterprise organization can benefit as the version is found to be systematically capable of clearly, completely and comprehensively modelling risk and security-related elements. This is validated by comparing an established model that follows the original version of the RSO [1] to the created incident model based on the redesigned version [6], [9] of the RSO.

To conclude, understanding the analysis of the determined risk and security limitations of the original RSO [1], the introduction of new ArchiMate elements, the redesigned concepts, and the concept of mutual activation strongly allow one to see why the redesigned version [6], [9] of RSO is more effective in displaying how organizations effectively visualize implemented security measures mitigating or preventing threat related elements. Hence, the redesigned approaches combined with the mutual activation concept are concluded to enable organizations to efficiently perform thorough risk, security, and gap analyses temporally on their processes allowing them to study and mitigate possible risks and threats effectively.

ACKNOWLEDGMENTS

In this section, the author of this research paper would like to express gratitude to his assigned research project supervisor Ítalo José da Silva Oliveira. The research project supervisor's constant support, feedback, and knowledge sharing related to risk and security modelling in enterprise architecture were invaluable to the success of this research in a limited amount of time. He did put significant effort into explaining the overall RSO concepts, the meanings of risk and security-related elements, and provided a comprehensible understanding of the interconnections between the covered elements in the data breach incident model. This was achieved through regular meetings, continuous constructive feedback and his patience.

REFERENCES

[1] I. Band, W. Engelsman, C. Feltus, S.G. Paredes, J. Hietala, H. Jonkers, and et al. 2017. *How to Model Enterprise Risk Management and Security with the ArchiMate Language.* Technical Report W172. The Open Group.

[2] Riccardo Baratella, Mattia Fumagalli, Ítalo Oliveira, and Giancarlo Guizzardi. 2022. Understanding and Modeling Prevention. In *Research Challenges in Information Science*, Renata Guizzardi, Jolita Ralyté, and Xavier Franch (Eds.). Springer International Publishing, Cham, 389–405.

[3] Gudmund Grov, Federico Mancini, and Elsie Margrethe Staff Mestl. 2019. Challenges for Risk and Security Modelling in Enterprise Architecture. In *The Practice of Enterprise Modeling*, Jaap Gordijn, Wided Guédria, and Henderik A. Proper (Eds.). Springer International Publishing, Cham, 215–225.

[4] Nicolas Mayer and Christophe Feltus. 2017. Evaluation of the risk and security overlay of archimate to model information system security risks. In *2017 IEEE*

21st International Enterprise Distributed Object Computing Workshop (EDOCW). 106–116. https://doi.org/10.1109/EDOCW.2017.30

[5] Microsoft. 2021. Analyzing Attacks Taking Advantage of the Exchange Server Vulnerabilities. https://www.microsoft.com/en-us/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/ Accessed: 2024-06-23.

[6] Ítalo Oliveira, Tiago Prince Sales, João Paulo A. Almeida, Riccardo Baratella, Mattia Fumagalli, and Giancarlo Guizzardi. 2024. Ontology-based security modeling in ArchiMate. *Software and systems modeling* (16 Feb. 2024). https://doi.org/10.1007/s10270-024-01149-1 Publisher Copyright: © The Author(s) 2024..

[7] Ítalo Oliveira, Tiago Prince Sales, Riccardo Baratella, Mattia Fumagalli, and Giancarlo Guizzardi. 2022. An Ontology of Security from a Risk Treatment Perspective. In *Conceptual Modeling (Lecture Notes in Computer Science)*, Jolita Ralyté, Sharma Chakravarthy, Mukesh Mohania, Manfred A. Jeusfeld, and Kamalakar Karlapalem (Eds.). Springer Nature, Switzerland, 365–379. https://doi.org/10.1007/978-3-031-17995-2_26 41st International Conference on Conceptual Modeling, ER 2022, ER 2022 ; Conference date: 17-10-2022 Through 20-10-2022.

[8] Alexis M Pitney, Spencer Penrod, Molly Foraker, and Suman Bhunia. 2022. A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities. In *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*. 1–6. https://doi.org/10.23919/SpliTech55088.2022.9854268

[9] Tiago Prince Sales, João Paulo A. Almeida, Sebastiano Santini, Fernanda Baião, and Giancarlo Guizzardi. 2018. Ontological Analysis and Redesign of Risk Modeling in ArchiMate. In *2018 IEEE 22nd International Enterprise Distributed Object Computing Conference (EDOC)*. 154–163. https://doi.org/10.1109/EDOC.2018.00028

[10] Tiago Prince Sales, Fernanda Baião, Giancarlo Guizzardi, João Paulo A. Almeida, Nicola Guarino, and John Mylopoulos. 2018. The Common Ontology of Value and Risk. In *Conceptual Modeling*, Juan C. Trujillo, Karen C. Davis, Xiaoyong Du, Zhanhuai Li, Tok Wang Ling, Guoliang Li, and Mong Li Lee (Eds.). Springer International Publishing, Cham, 121–135.

[11] TechUK. 2021. Top Tips to Protect Against the Microsoft Exchange Server Hack. https://www.techuk.org/resource/top-tips-to-protect-against-the-microsoft-exchange-server-hack.html Accessed: 2024-06-23.

A APPENDIX A: MICROSOFT EXCHANGE SERVER DATA BREACH INCIDENT MODEL IN ARCHIMATE

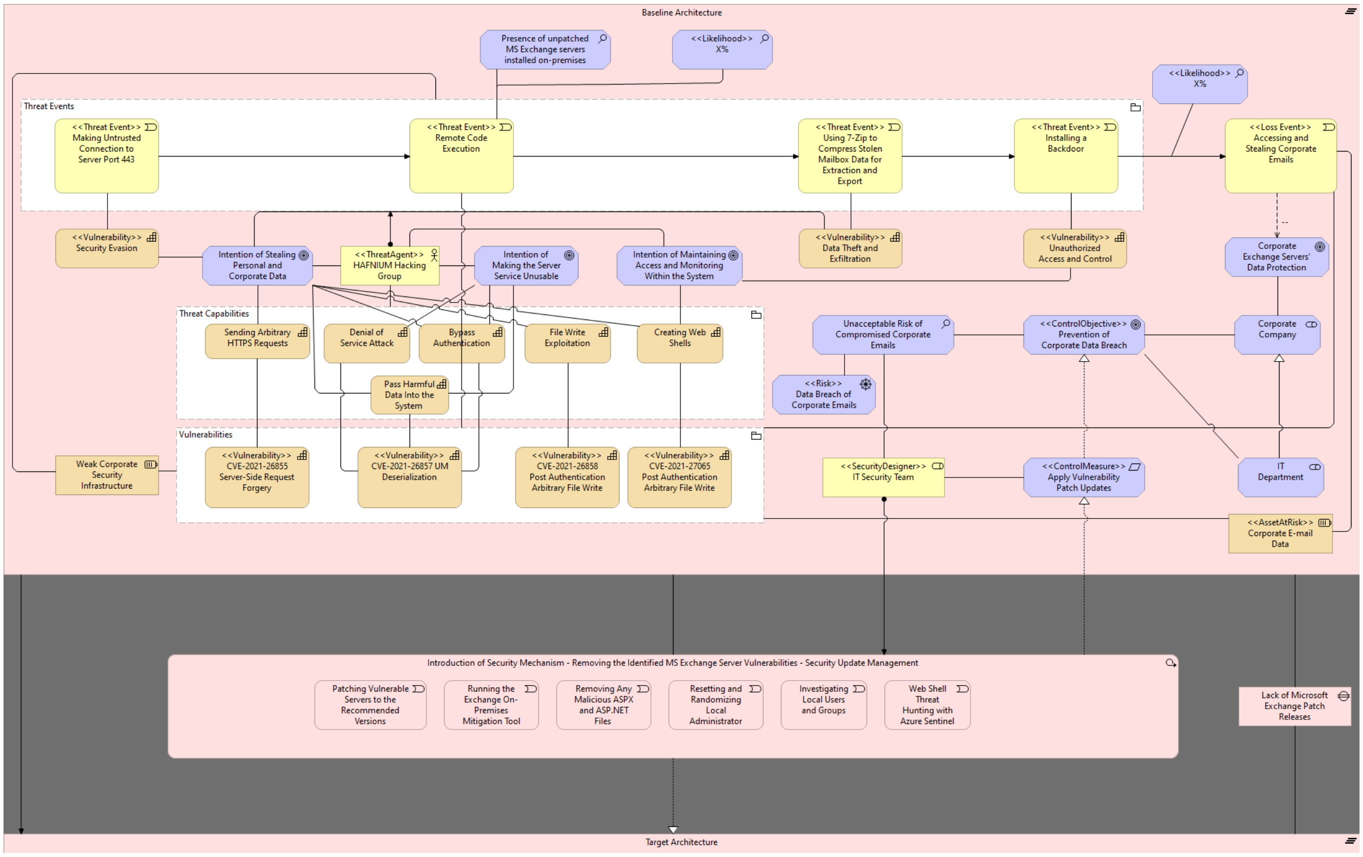
Baseline Architecture
Presence of unpatched MS Exchange servers installed on-premises
<<Likelihood>> X%
<<Likelihood>> X%
Threat Events
<<Threat Event>> Making Untrusted Connection to Server Port 443
<<Threat Event>> Remote Code Execution
<<Threat Event>> Using 7-Zip to Compress Stolen Mailbox Data for Extraction and Export
<<Threat Event>> Installing a Backdoor
<<Loss Event>> Accessing and Stealing Corporate Emails
<<Vulnerability>> Security Evasion
Intention of Stealing Personal and Corporate Data
<<ThreatAgent>> HAFNIUM Hacking Group
Intention of Making the Server Service Unusable
Intention of Maintaining Access and Monitoring Within the System
<<Vulnerability>> Data Theft and Exfiltration
<<Vulnerability>> Unauthorized Access and Control
Corporate Exchange Servers' Data Protection
Threat Capabilities
Sending Arbitrary HTTPS Requests
Denial of Service Attack
Bypass Authentication
File Write Exploitation
Creating Web Shells
Pass Harmful Data Into the System
Unacceptable Risk of Compromised Corporate Emails
<<ControlObjective>> Prevention of Corporate Data Breach
Corporate Company
<<Risk>> Data Breach of Corporate Emails
Vulnerabilities
Weak Corporate Security Infrastructure
<<Vulnerability>> CVE-2021-26855 Server-Side Request Forgery
<<Vulnerability>> CVE-2021-26857 UM Deserialization
<<Vulnerability>> CVE-2021-26858 Post Authentication Arbitrary File Write
<<Vulnerability>> CVE-2021-27065 Post Authentication Arbitrary File Write
<<SecurityDesigner>> IT Security Team
<<ControlMeasure>> Apply Vulnerability Patch Updates
IT Department
<<AssetAtRisk>> Corporate E-mail Data
Introduction of Security Mechanism - Removing the Identified MS Exchange Server Vulnerabilities - Security Update Management
Patching Vulnerable Servers to the Recommended Versions
Running the Exchange On-Premises Mitigation Tool
Removing Any Malicious ASPX and ASP.NET Files
Resetting and Randomizing Local Administrator
Investigating Local Users and Groups
Web Shell Threat Hunting with Azure Sentinel
Lack of Microsoft Exchange Patch Releases
Target Architecture

Fig. 2. Baseline Architecture and Introduction of Security Mechanism

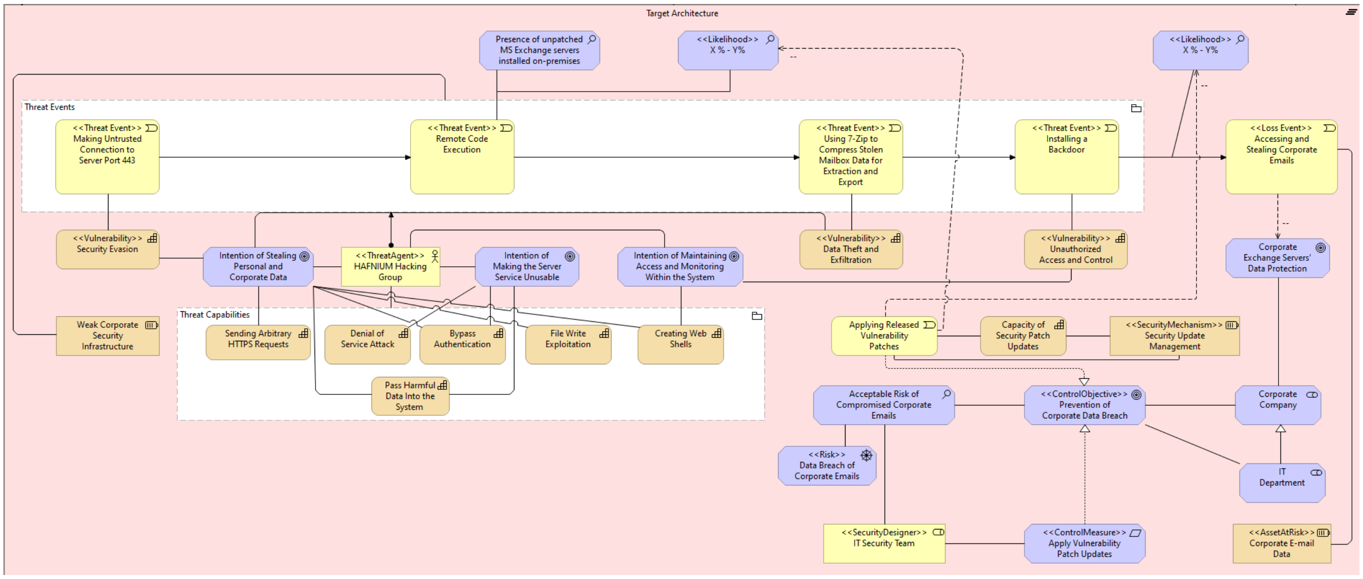
Target Architecture
Presence of unpatched MS Exchange servers installed on-premises
<<Likelihood>> X % - Y%
<<Likelihood>> X % - Y%
Threat Events
<<Threat Event>> Making Untrusted Connection to Server Port 443
<<Threat Event>> Remote Code Execution
<<Threat Event>> Using 7-Zip to Compress Stolen Mailbox Data for Extraction and Export
<<Threat Event>> Installing a Backdoor
<<Loss Event>> Accessing and Stealing Corporate Emails
<<Vulnerability>> Security Evasion
Intention of Stealing Personal and Corporate Data
<<ThreatAgent>> HAFNIUM Hacking Group
Intention of Making the Server Service Unusable
Intention of Maintaining Access and Monitoring Within the System
<<Vulnerability>> Data Theft and Exfiltration
<<Vulnerability>> Unauthorized Access and Control
Corporate Exchange Servers' Data Protection
Weak Corporate Security Infrastructure
Threat Capabilities
Sending Arbitrary HTTPS Requests
Denial of Service Attack
Bypass Authentication
File Write Exploitation
Creating Web Shells
Pass Harmful Data Into the System
Applying Released Vulnerability Patches
Capacity of Security Patch Updates
<<SecurityMechanism>> Security Update Management
Acceptable Risk of Compromised Corporate Emails
<<ControlObjective>> Prevention of Corporate Data Breach
Corporate Company
<<Risk>> Data Breach of Corporate Emails
IT Department
<<SecurityDesigner>> IT Security Team
<<ControlMeasure>> Apply Vulnerability Patch Updates
<<AssetAtRisk>> Corporate E-mail Data

Fig. 3. Target Architecture