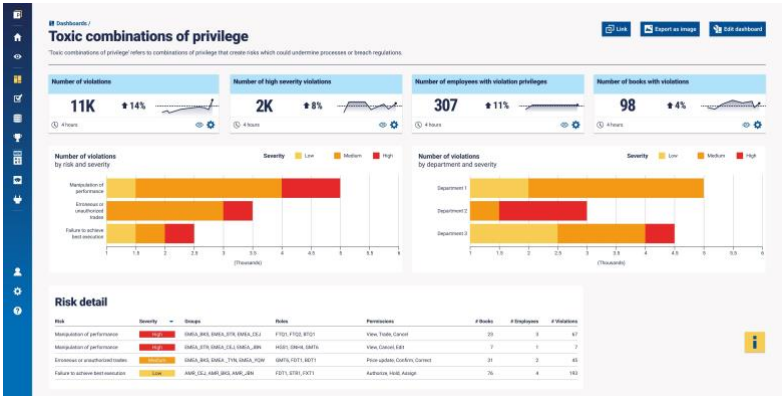
5 Quick wins to manage insider threats.

Quick Wins to reduce risks due to Toxic Combinations

Pr. Nsiangani, Expert Information Security & Cyber Defense



Introduction

. Toxic combinations in financial services companies refer to the risks that can arise when certain combinations of people, processes, and technologies come together in a way that creates negative consequences. These toxic combinations can take many different forms, but often involve a combination of IT systems, processes, and human behavior that creates vulnerabilities or exposes the company to risks.

In this white paper, we will explore the types of toxic combinations that can occur in financial services companies, the risks that these combinations pose, and the steps that companies can take to address these risks. We will begin by providing an overview of the types of toxic combinations that can occur in IT systems, and the risks that these combinations pose. We will then explore the problems and risks associated with toxic combinations in financial services companies, and provide a detailed solution section that outlines the steps that companies can take to address these risks.

Toxic combinations in financial services companies can have serious consequences, including financial losses, reputational damage, and regulatory penalties. By understanding the types of toxic combinations that can occur and the risks that these combinations pose, companies can take steps to address these risks and protect themselves against the potential consequences of toxic combinations. In this white paper, we will provide a detailed overview of the types of toxic combinations that can occur in financial services companies, the problems and risks that these combinations pose, and the steps that companies can take to address these risks. So, it is important for financial services companies to understand and address toxic combinations in order to protect themselves and their stakeholder

The Problem and Risks:

In financial services companies, toxic combinations can take many different forms and can involve a range of people, processes, and technologies. Some common types of toxic combinations that can occur in financial services companies include:

Complex IT systems: Financial services companies often rely on complex IT systems to support their operations, and these systems can be vulnerable to toxic combinations. For example, if a company has multiple systems that are not properly integrated or are poorly designed, this can create vulnerabilities that may be exploited by attackers or insiders.

Ineffective processes: Toxic combinations can also occur when processes are not properly designed or are not followed consistently. For example, if a company has

inadequate controls for access to sensitive information, this can create risks for data breaches or unauthorized access.

Human behavior: Toxic combinations can also involve human behavior, such as when employees or contractors engage in risky or inappropriate behavior. For example, if employees have access to sensitive information but are not properly trained on how to handle this information, they may be more likely to make mistakes or engage in risky behavior.

These toxic combinations can pose significant risks to financial services companies, including financial losses, reputational damage, and regulatory penalties. To better understand the risks and challenges associated with toxic combinations in financial services companies, it can be helpful to consider specific scenarios. Below, we will outline three scenarios for toxic combinations in financial services companies, including their vulnerability, attack vector, risk, severity, and likelihood:

Scenario 1: A financial services company has multiple systems that are not properly integrated, which creates vulnerabilities that are exploited by an attacker.

Vulnerability: The company's IT systems are not properly integrated, creating vulnerabilities that can be exploited.

Attack vector: An attacker exploits these vulnerabilities to gain unauthorized access to sensitive information or systems.

Risk: High, as the attacker has access to sensitive information or systems and may use this access to cause damage or steal sensitive data.

Severity: High, as a data breach or unauthorized access to systems can lead to significant financial and reputational damage for the company.

Likelihood: Moderate to high, depending on the complexity and integration of the company's IT systems and the sophistication of the attacker.

Scenario 2: A financial services company has inadequate controls for access to sensitive information, which leads to a data breach.

Vulnerability: The company has inadequate controls for access to sensitive information.

Attack vector: An employee or contractor with access to sensitive information intentionally or unintentionally misuses this information, resulting in a data breach.

The Solution

To effectively address toxic combinations in financial services companies, it is important to adopt a proactive and comprehensive approach. This may involve a range of measures, including technical controls, policies and procedures, and human behavior interventions. Below, we

will outline three easy mitigations that financial services companies can take to address toxic combinations and reduce the risks that these combinations pose:

Review and update IT systems: One of the most effective ways to reduce the risk of toxic combinations in IT systems is to regularly review and update these systems. This may involve conducting audits or assessments of the company's IT systems to identify vulnerabilities or areas for improvement, and implementing changes to address these vulnerabilities. For example, companies may need to update their systems to ensure that they are properly integrated and secure, or may need to implement additional controls to prevent unauthorized access to sensitive information. By regularly reviewing and updating their IT systems, financial services companies can reduce the risk of toxic combinations and protect themselves against the potential consequences.

Establish strong policies and procedures: Another key step in addressing toxic combinations is to establish strong policies and procedures that outline the expectations and responsibilities of employees, contractors, and business

partners. These policies and procedures should cover a wide range of topics, including data security, information access, and incident reporting, and should be regularly reviewed and updated to ensure that they remain effective and relevant. By establishing clear policies and procedures, financial services companies can provide guidance to employees and other stakeholders and help to prevent toxic combinations from occurring.

Implement human behavior interventions: To address toxic combinations that involve human behavior, financial services companies may need to implement human behavior interventions. This may include training programs to educate employees and contractors about the risks and consequences of toxic combinations, as well as programs to encourage ethical behavior and discourage risky or inappropriate behavior. By implementing these interventions, financial services companies can reduce the risk of toxic combinations and protect themselves against the potential consequences.

Overall, these three easy mitigations can help financial services companies to effectively address toxic

combinations and reduce the risks that these combinations pose. By reviewing and updating their IT systems, establishing strong policies and procedures, and implementing human behavior interventions, financial services companies can take a proactive and comprehensive approach to tackling toxic combinations and protecting themselves against the potential consequences.

To implement these mitigations effectively, it is important for financial services companies to follow a structured and systematic approach. Below, we will outline step-by-step instructions for each of these mitigations:

Review and update IT systems:

Step 1: Conduct an audit or assessment of the company's IT systems to identify vulnerabilities or areas for improvement.

Step 2: Develop a plan to address identified vulnerabilities or areas for improvement, including a timeline and budget.

Step 3: Implement the plan, including any necessary updates to the company's IT systems.

Step 4: Test the updated systems to ensure that they are functioning properly and meeting the company's needs.

Step 5: Regularly review and update the company's IT systems to ensure that they remain secure and effective.

Establish strong policies and procedures:

Step 1: Identify the key areas where strong policies and procedures are needed, such as data security, information access, and incident reporting.

Step 2: Develop draft policies and procedures for these areas.

Step 3: Review and revise the draft policies and procedures as needed.

Step 4: Communicate the policies and procedures to employees, contractors, and business partners.

Step 5: Monitor compliance with the policies and procedures and make any necessary updates to ensure that they remain effective and relevant.

Implement human behavior interventions:

Step 1: Identify the key areas where human behavior interventions are needed, such as training programs or programs to encourage ethical behavior.

Step 2: Develop a plan for implementing these interventions, including a timeline and budget.

Step 3: Implement the plan, including any necessary training programs or other interventions.

Step 4: Monitor the effectiveness of the interventions and make any necessary updates or adjustments.

Step 5: Regularly review and update the interventions to ensure that they remain effective and relevant.

By following these step-by-step instructions, financial services companies can effectively implement the three easy mitigations outlined above and take a proactive and comprehensive approach to addressing toxic combinations. By adopting this approach, financial services companies can reduce the risk of toxic combinations and protect themselves against the potential consequences

Conclusion:

In conclusion, toxic combinations in financial services companies can have serious consequences, including financial losses, reputational damage, and regulatory penalties. These toxic combinations can take many forms, including complex IT systems, ineffective processes, and human behavior, and can pose significant risks to the company.

To effectively address toxic combinations, financial services companies must adopt a proactive and comprehensive approach that involves regularly reviewing and updating IT systems, establishing strong policies and procedures, and implementing human behavior interventions. By following these recommendations, financial services companies can reduce the risk of toxic combinations and protect themselves against the potential consequences.

It is important for financial services companies to understand and address toxic combinations in order to protect themselves and their stakeholders. By taking a proactive and comprehensive approach to addressing these risks, financial services companies can reduce the risk of

toxic combinations and protect themselves against the potential consequences..