Mitigating Insider Threats: Insights from Software Security Experts for Process Improvement and Risk Reduction

Azzah Alghamdi[1], Mahmood Niazi[2], Lucas Cordeiro[3], Mamoona Humayun[4], Andrew Stewart[3]

[1] Computer Information Systems Department, College of Computer Science and Information Technology, Imam Abdalrhman Bin Faisal University, Saudi Arabia

[2] Department of Information and Computer Science, Interdisciplinary Research Centre for Intelligent Secure Systems, King Fahd University of Petroleum and Minerals, Saudi Arabia

[3] Department of Computer Science, University of Manchester, United Kingdom

[4] School of Arts, Humanities and Social Sciences, University of Roehampton, London, United Kingdom

APPENDIX (A) A list of the best practices to mitigate insider threats

Code	Practice
Compliance best practices	
CP1	Recognize dangerous actors and act quickly when you see something off.
CP2	Policies and regulations should be documented and regularly enforced.
CP3	Provide physical security for the workplace.
CP4	Limit access from third parties.
CP5	Clearly state all cloud services' security terms, including monitoring and access limits.
CP6	Characteristics of people most prone to jeopardize assets.
CP7	Determine the cross-functional participants.
CP8	Handle and evaluate interested parties.
CP9	Observe this rule: "If You See Something, Say Something."
Human resources best practices	
HR1	All staff should receive frequent security training that covers insider threat knowledge.
HR2	Create a thorough approach for terminating employees.
HR3	Run background checks on staff members, especially those needing sensitive data access.
HR4	Using Simulators for Cyber Threat Awareness.
HR5	Offer Jobs with Assistance Program (EAP).
HR6	Keep employees' values and attitudes in line with the principles and mission of the company.
Top management best practices	
TM1	Create a plan for responding to insider incidents.
TM2	Determine which assets are in danger.
TM3	Create a structured insider threat mitigation program.
TM4	Recognize and safeguard important assets.
TM5	Turn on the surveillance.
TM6	Continuous monitoring.
TM7	Conduct a persona analysis of insider threats.
TM8	Turn "Sentiment Analysis" on.
TM9	Ensure a certain employee has access to the organization's vital resources.
TM10	Consider and prepare for "Typical" inquiries.
TM11	Create a threat management team to handle assessment, handling, and responding.
TM12	Sync up HR and IT security.
TM13	Make documentation or a checklist for controlling insider threats.
TM14	Create new indicators by utilizing previous insider cases.
TM5	In the event of an insider incident, the department manager is required to report to management.
TM16	To reduce insider stress and errors, organize tasks and management.
TM17	Use motivating rewards to synchronize employees with the company.
TM18	Examine the programs
Technical best practices	
IT1	Establish stringent procedures and guidelines for password and account management.
IT2	Enforce the least privilege and the division of obligations.
IT3	Put in place safe procedures for recovery, archiving, and backup.
IT4	Make use of DLP, or data loss prevention.
IT5	Exercise Caution with System Administrators and Technical Users.
IT6	To log in, use a security information and event management system (SIEM) or log correlation engine.
IT7	Tracking, auditing, and logging internet activities of staff
IT8	For high-risk data, create a policy for data handling and classification and make use of data loss technologies.
IT9	Install appliances and software for security.
IT10	Keep an eye on and manage remote access from every endpoint.
IT11	Put robust authentication into practice.
IT12	Cease the exfiltration of data.
IT13	Analyze and carefully consider requests for more access to the system or network.
IT14	Make use of NTI, or network traffic intelligence.
IT15	Properly recycle outdated hardware and documentation.
IT16	Employ methods for detecting intrusions.
IT17	Control the risk posed by shared passwords.
IT18	Implement systems to keep an eye on workers' activities and link data from various sources.
IT19	If there is an IT security compromise, do precise IT forensics.
IT20	Identify compromised accounts.
IT21	Find and prevent misuse of privileged access.
IT22	Stop logic bombs from going off.
IT23	Establish stringent data access rules to ensure that staff members can only view the information they need.
IT24	Even in cases where credentials are misplaced, pilfered, or exploited, prevent unwanted access.
IT25	Eliminate inactive and abandoned accounts.
IT26	Establish clear guidelines for the use, sharing, and storing of data when allowing people to bring their own devices (BYOD).
IT27	To restrict the usage of personal devices and information sharing outside of your company network, set up network access rules.
IT28	Make use of biometric technology.

IT29	Recognize the dangers that face IT infrastructure today.
IT30	Refrain from logging onto the system outside of business hours or on holidays unless specifically authorized by a higher-ranking individual.
IT31	Keep the technical room locked, and only permit entry with the approval of a higher-ranking staff member and while the staff member is present.
IT32	Gather and combine different data sources.
IT33	Managing private data in an appropriate manner that is necessary for an insider threat audit.
IT34	Administer conduct guidelines to all users and place banners on all platforms.

APPENDIX (B) List of SLR sources

No.	Title	Year	Source
1	"Best Practices against Insider Threats in All Nations".	2012	IEEE Technical note
2	"Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures".	2019	ACM Journal
3	"Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures".	2007	John Wiley & Sons Book
4	"Insider threats of Physical Protection Systems in Nuclear Power Plants: Prevention and Evaluation".	2018	Science Direct Article
5	"An Insider Threat Factors and Features Categorization for Manufacturing Execution System".	2020	Springer Lecture Notes inside a Book
6	The Insider.	2012	John Wiley & Sons Book Chapter
7	"Intentions to Comply versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders".	2018	John Wiley & Sons Article
8	"Information Security: Examining and Managing the Insider Threat".	2006	ACM Conference
9	"Insider Threat Assessment: A Model-Based Methodology".	2014	ACM Research Paper
10	Insider Threat Program Best Practices.	2013	IEEE Conference
11	"Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies."	2014	IEEE Conference
12	"Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures".	2019	ACM Journal
13	"Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures".	2007	John Wiley & Sons Book Appendix
14	Aspects of Insider Threats.	2010	Springer Book Chapter
15	"Insider Threat and Information Security Management".	2010	Springer Book Chapter
16	"Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation".	2010	Springer Book Chapter
17	"Insider Attack and Cyber Security: Beyond the Hacker."	2008	Springer Book Chapter
18	Insider Threat.	2017	Science Direct Book Chapter
19	"Combating the Insider Cyber Threat".	2008	IEEE Article
20	"Beyond Accountability: Using Obligations to Reduce Risk Exposure and Deter Insider Attacks".	2013	ACM Research Article
21	"Threat from Within: Case Studies of Insiders Who Committed Information Technology Sabotage".	2016	IEEE Conference
22	"A Framework of Opportunity-Reducing Techniques to Mitigate the Insider Threat".	2015	IEEE Conference
23	"The Insider Threat: Reasons, Effects and Mitigation Techniques".	2020	ACM Conference
24	"Insider Threats in Information Security Categories and Approaches."	2015	IEEE Conference