Realtime publishers

Monitoring, Detecting and Preventing Insider Fraud and Abuse

Dan Sullivan

sponsored by

Attachmate

Copyright Statement

Chapter 4: Selecting the Right Tools: Evaluating Applications for Monitoring, Preventing, and Investigating Insider Abuse

The threat of insider abuse and the potential costs of that threat are more than enough to motivate businesses to implement fraud controls. We saw in Chapter 2 that technical barriers have historically hindered efforts to block insider fraud. Factors such as the legitimate access to applications and data, insider knowledge, and the ability to tamper with access controls limit the effectiveness of security controls that were designed to protect against outsiders. Although we are not helpless when it comes to insider abuse, we need a different set of controls than those used to protect from outside attack. As discussed in Chapter 3, techniques such as multi-channel monitoring and application activity analysis provide the foundation for detecting, blocking, and investigating insider abuse. Here in Chapter 4, the final chapter of this book, we will examine how to evaluate and select tools for controlling insider abuse.

This chapter structures the evaluation process around three areas:

- Functional requirements
- Non-functional requirements
- Support for compliance practices

Functional requirements are made up of key business and technical requirements for support of particular features. Consider the fact that insider fraud can take on different forms in different industries. Fraud in an insurance company will look different from fraud in a commercial bank or manufacturing plant. Clearly, we will need the ability to define industry-specific rules about legitimate and illegitimate application activity. A common technical requirement is the need to support multiple platforms. Heterogeneous IT environments are the norm, and insider fraud systems will have to operate across these various platforms.

Non-functional requirements address features of a system that are not isolated to the ability for a user or application administrator to carry out a particular operation within a system. For example, insider fraud prevention tools should be scalable. As the number of inter-operating applications and the number of users grows, the insider fraud system should be able to keep pace with the growing volume of activity data that must be monitored.

Support for compliance practices represents an important subset of functional and non-functional requirements, and encompasses topics such as integrating an insider abuse control system with policies and procedures and using such a system to support forensic investigations. Although this topic subset would certainly fit within the discussion of functional and non-functional requirements, support for compliance is such an essential component in the long-term success of an insider abuse control system that it warrants a separate discussion.

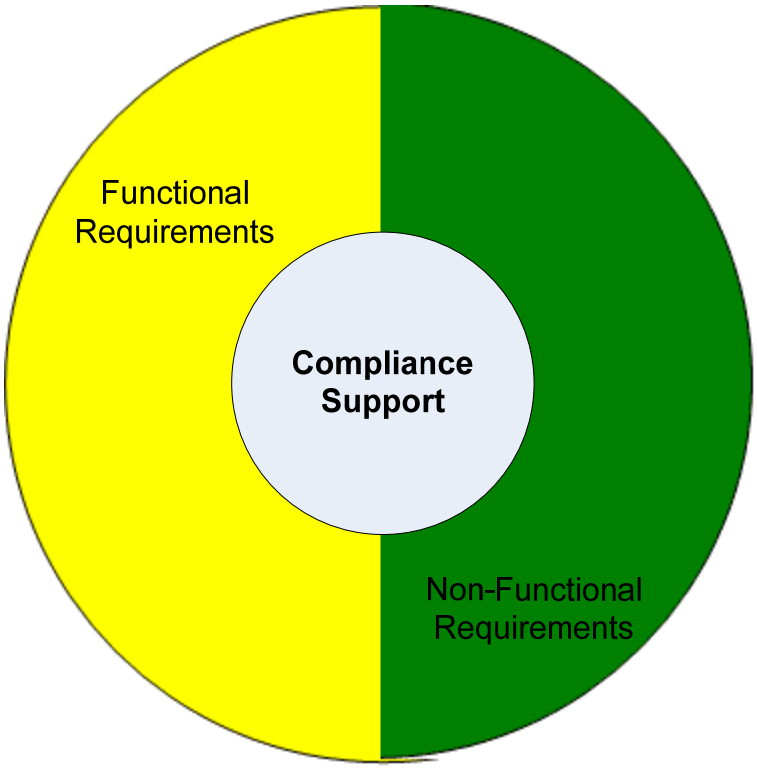

Figure 4.1: Evaluation of insider abuse control applications should be based on a combination of functional and non-functional requirements with particular attention to compliance support.

Key Functional Requirements

The functional requirements of an insider abuse control system can be divided into business requirements and technical requirements.

Business Functional Requirements

Business functional requirements are features that make an application a good fit for solving well-defined business needs. Given the complexity of insider fraud, it is not surprising that the business requirements will be broad and sometimes complicated, at least at some level.

Also, the specific implementation details for meeting business requirements will vary by industry and use cases. For example, rules for detecting fraud in an investment bank will be specific to investment banking. For the purposes of our discussion, we will not delve into industry-specific details but examine key functional business requirements at a more general level.

Three functional business requirements are broadly relevant across industries and use cases. These business requirements address needs for industry-specific heuristics, usable interfaces by fraud/security professionals, and configurable heuristics for business-specific needs. Insider fraud control applications that meet these three requirements will be both relevant to and usable by businesses that need them.

Industry-Specific Heuristics

In many ways, insider fraud is the same crime no matter how it is perpetrated. Some combination of deceit and theft leave a business victimized by an insider. It is probably useful to think in terms of this general level when dealing with legal aspects of fraud, such as how to prosecute a case against an insider who has committed fraud. It is also useful from a risk management perspective when trying to understand the potential costs of insider fraud and the role of insurance or other risk mitigation strategies. It is not, however, sufficient for controlling insider abuse.

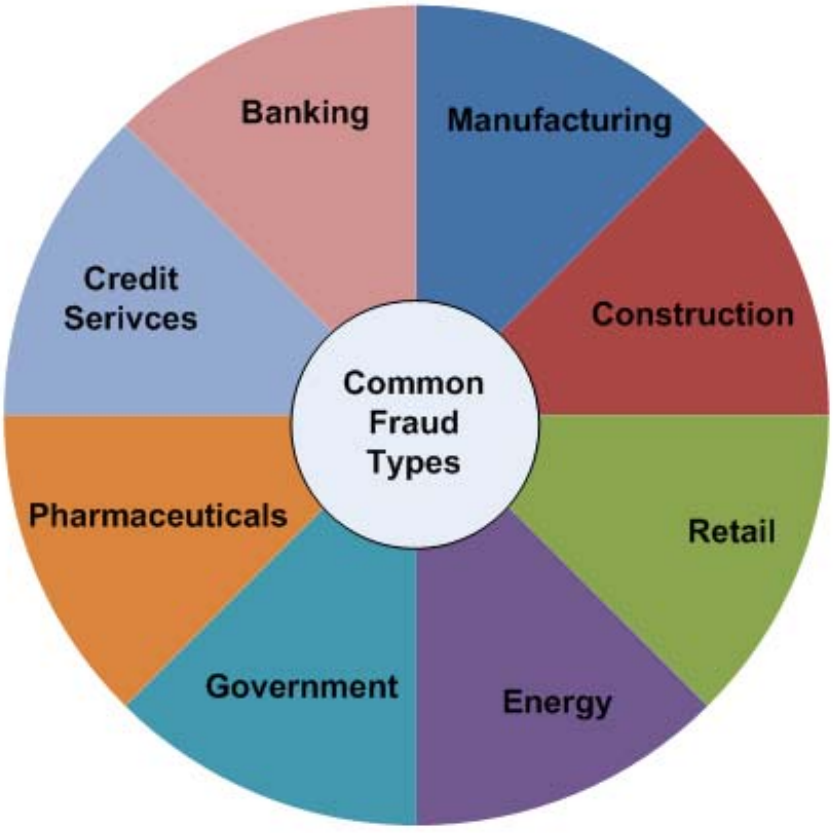

Figure 4.2: Fraud can be committed in different ways across different industries, although common forms do exist.

To control insider abuse, we must take into account the details of how fraud is executed. Fraud may target a business process, such as accounts payable or customer refund procedures. These procedures may be very similar even in dissimilar industries. After all, a bank pays for office supplies and shipping services in much the same way a pharmaceutical company would. Fraud that targets common business processes can be detected across industries using a common set of rules and pattern-detection algorithms with minimal customization. Examples of common business process and procedures include:

- Accounts payable
- Accounts receivable
- Inventory control
- Payroll

As we move away from common business procedures, there is greater need for industry-specific heuristics for detecting fraud. Consider some examples of industry-specific fraud:

- An employee of a credit card company works with identity thieves to tamper with the customer profiles associated with fraudulent cards to minimize the chance transactions will be declined by risk assessment systems.
- A mortgage processor in a commercial bank receives kickbacks from a third-party mortgage originator in return for falsifying records to bypass underwriting procedures and ensure risky mortgages are underwritten.
- An engineer at an electronic manufacturer steals design documents related to a new product line before leaving the company to join a competitor.
- A clerk in a medical records processing department uses his access to confidential patient data to collect information on public figures and sell that information to disreputable media outlets.

These examples of fraud are different from attacks against business financial systems. The industry-specific fraud examples target workflow and business procedures underlying core business operations. Insider abuse detection will depend on the ability to create patterns for detecting activities that are indicative of a specific type of fraud.

In the case of the employee in the credit card company, we might need heuristics for monitoring changes to customer credit profiles and buying patterns. Employees who make an unusually large number of changes to customer profiles may require further monitoring. A bank providing mortgages may monitor the percentage of loans processed by a processor that originated with a particular third party. Cases in which an originator's loans are frequently processed by one may indicate possible collusion.

Companies with significant investments in intellectual property need to protect that with a significant investment. In such cases, there is a greater need to monitor file systems, email servers, and other collaboration tools that are used to store and exchange unstructured data, such as documents and design plans.

Industries such as health care and government are required to collect and maintain significant amounts of personally identifiable information. In such situations, insiders may be tempted to view and possibly sell confidential details about patients and citizens. In these cases, insider fraud control systems should be able to monitor patterns such as unusually frequent access of databases containing private information or access of information outside an employee's area of responsibility.

Application usability is one business requirement that spans industries.

Usability for Fraud and Security Professionals

Just as we do not need to be automotive mechanics to drive a car, fraud prevention and security professionals should not have to be programmers or systems administrators in order to use an insider fraud control system. Several usability factors are especially important in insider fraud control systems:

- Ability to assess various high-level activity indicators
- Ability to drill down into the details of any suspicious activity
- Comparative metrics for key activities, for example, cash outlays, incomplete purchase transactions, large numbers of small transactions involving the same vendor, supplier, or buyer
- Ability to define triggers that alert the user when an event occurs or some threshold is passed
- Ability to navigate between different types of information without rigid or complex steps

Ideally, an insider fraud control system will provide security professionals with a high-level view of activities on a particular system or set of systems. Details about the number of users currently using an application, the types of operations being performed, and the set of activities in which a key metric falls outside of a normal range can all help focus the security professional on areas that need attention. For example, if the past 24-hour period has seen a significant increase in the number of new customer accounts created, a fraud professional might want to drill down into details about the distribution of those new accounts. Were they created by a number of account representatives, as we would expect if this were the result of a new promotion or marketing campaign? Or were they primarily created by a single employee?

Comparative statistics are also necessary for many kinds of assessments. If a customer service representative has updated 60 customer credit profiles in the past week, is that unusual? We should compare that rate with rates of other representatives with comparable responsibilities and access privileges to get a better sense of what is typical and expected.

Fraud detection is in part an exploratory process. Professionals look for metrics of business procedures that indicate unusual levels of activity as well as patterns of activity that are indicative of fraudulent acts. Both of these are the kinds of events that can be continuously monitored. When a suspicious pattern of activity occurs or a threshold is passed, an alert can be sent to a fraud professional. Alerts can save fraud professionals from tedious or repetitive tasks and leave those professionals with more time for more interesting and productive types of analysis.

Navigation is another key to usability. A fraud prevention professional may be looking at one set of metrics and have a hunch that requires her to consider a different set of data. The system should be designed to facilitate, or at least not hinder, the rapid transition from one part of the system to another. Rigid hierarchical navigations schemes can slow the exploration and discovery process.

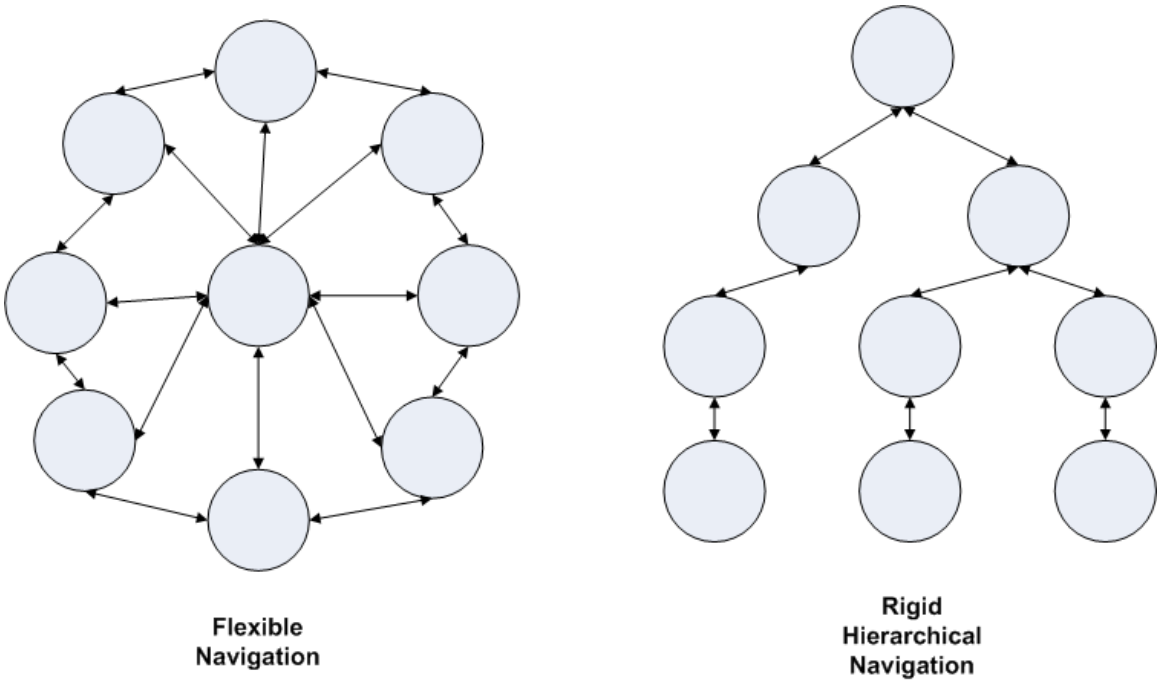

Figure 4.3: The ability to quickly navigate between different types of analysis and data sources facilitates exploratory discovery.

Configurable Heuristics for Business-Specific Needs

Another functional requirement we should consider is the need for configurable heuristics. An insider fraud control system will have heuristics for common types of fraud, such as those targeting core finance, and should have industry-specific heuristics. These heuristics represent a substantial investment on the part of the vendor providing the solution, but no matter how much effort they put into developing industry-specific rules for detecting fraud, customers should have the ability to customize fraud detection rules.

The combination of industry-specific heuristics, usability considerations, and the ability to customize heuristics to each business' specific requirements constitutes the core functional business requirements for an insider fraud control system. Another set of functional requirements center around the technical aspects of fraud detection and prevention.

Key Technical Requirements

Technical requirements stem from a combination of the nature of IT platforms and the needs of fraud prevention and security professionals. The basic technical requirements for an insider fraud control system are:

- Support for multiple platforms
- Real-time application activity monitoring
- Searchability across sessions
- Pattern analysis and reporting

Together, these provide the means for capturing data from multiple systems, analyzing it, and reporting it back to the professionals who can act on it.

Support for Multiple Platforms

Most business information technology platforms are heterogeneous. Even within small and midsized businesses, it is not uncommon to have a mix of platforms. In larger enterprises, there is a broader array of platforms and infrastructure that must be monitored. A typical enterprise-scale IT operation will support some or all of the following:

- Multiple generations of PCs and laptops
- Mobile devices
- Linux and Unix servers
- Windows servers
- Mainframes

Business processes often depend upon multiple platforms to deliver services. Even a relatively simple business service, such as email, will require servers running one operating system (OS) to provide email access to client devices including desktops, laptops and mobile phones. More complex business processes can include multi-tiered mainframe applications that write data to messaging queues which in turn deliver data to Linux servers where it's consumed by an application that provides back-end services to a Web application.

The various elements that go into an enterprise application allow for a great deal of flexibility from a design and deployment perspective, but they also provide opportunity to those seeking to commit fraud. Take for example a simple case of a Web application that collects information from a customer service representative and updates a customer account. The application sounds simple enough but there are several layers:

- A client interface running in a browser on a PC
- A Web server running on a Linux server
- A custom Java application running in an application server on a Linux server
- A relational database that stores the data long term

Each layer presents opportunities for executing fraud-related tasks (see Figure 4.4).

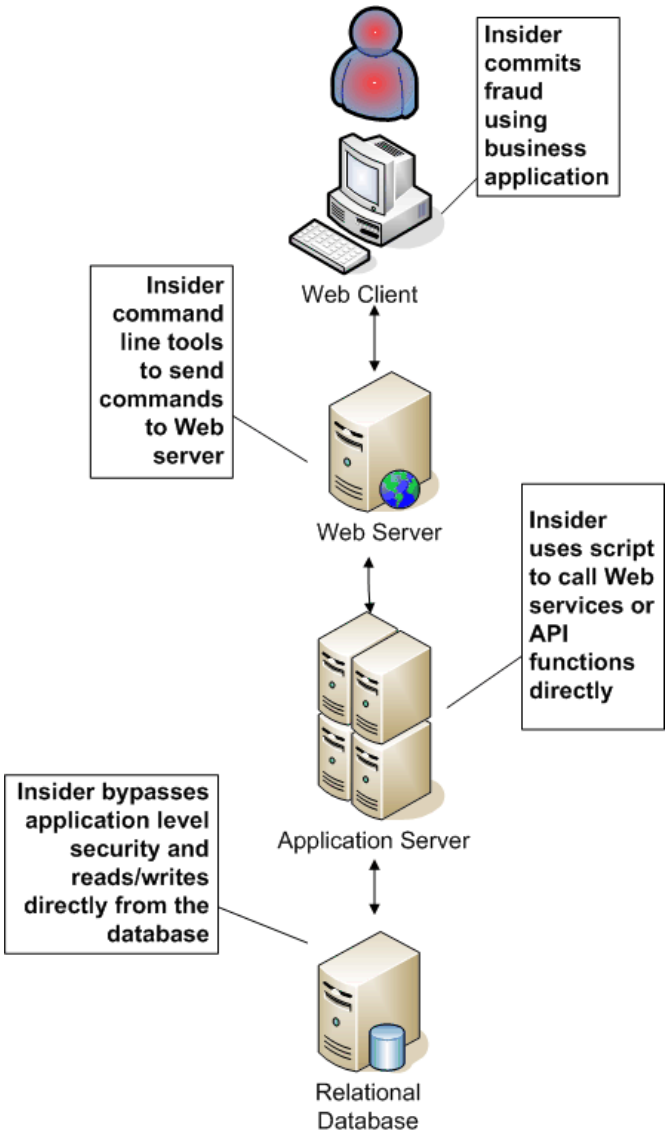

Figure 4.4: Insiders can use their access privileges to execute fraud-related actions at multiple layers of the application stack.

As Figure 4.4 shows, it is not sufficient to just monitor a Unix server hosting a relational database or track activities on Windows devices running Web browsers. Business applications are not monolithic; they run across multiple platforms and insider fraud control systems have to run across multiple platforms as well.

Realtime Application Activity Monitoring

Tampering with electronic records can occur within seconds. Insiders might be able to query and download hundreds of private and confidential records in a matter of minutes. A disgruntled employee could copy plans for a new product to a flash drive and be out the front door in a short period of time. Insider fraud control systems can support forensic investigations for after-the-fact analysis, and they can help identify suspicious patterns of activity, but to be the most use, they should do this in near real-time.

By actively collecting data on application activities and analyzing as fast as the data is generated, insider fraud control systems enable us to be in a position to rapidly respond and potentially block fraud as it occurs. For example, if an employee has performed read operations on an unusually large number of confidential records in the database and starts to run queries selecting data from a significant-sized set of confidential records, we may want to block those queries or even disable the employee's access. Another factor of effective data collection and analysis is the ability to rapidly find targeted information, such as related data across sessions.

Searching Across Sessions

Insiders do not necessarily commit fraud in a single session. Though that can happen, an unscrupulous insider might instead execute a multi-step plan devised to avoid detection by existing checks on isolated transactions. For example, an insider might execute five transactions over the course of a week after normal business hours to avoid the possibility of someone looking over his shoulder and seeing unusual activities.

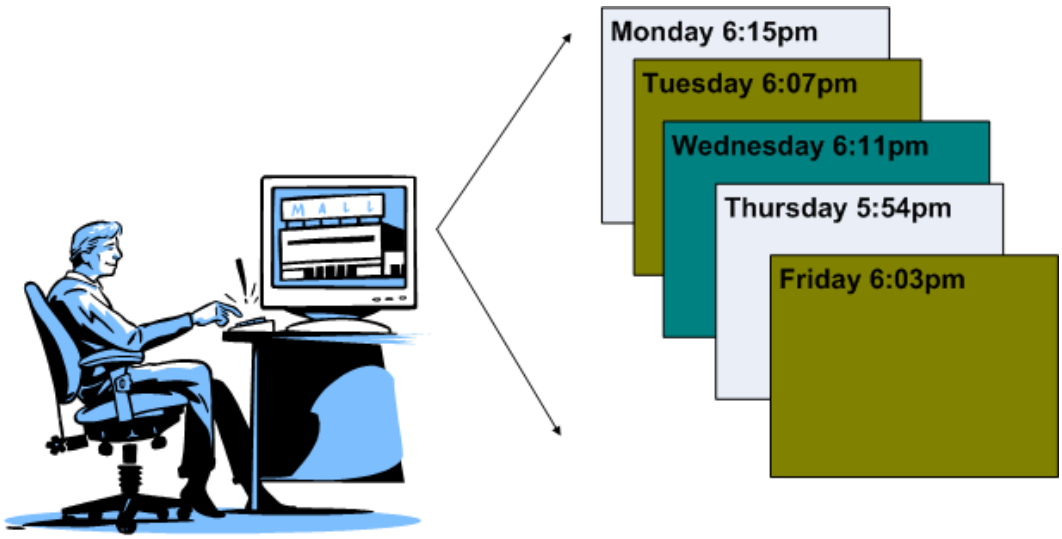

Figure 4.5: Isolated transactions may not be suspicious but when detected as a pattern across sessions with common attributes, the transactions may be indicative of fraudulent activity.

A fraud analyst might suspect an employee is disgruntled or having personal financial problems and that employee may attempt to commit fraud. The analyst will want to search across application sessions by attributes, such as sessions in which the employee is

- Logged into the application
- Using the application after normal business hours
- Performing an unusual sequence of commands within the application
- Logging off the application after running less than the average number of commands within that application

The analyst may want to search across sessions for other patterns of activity as well. The fraud analyst knows there is a weakness in the application controls, which creates a potential way for someone to trick the account management system into issuing payments when they are not required. For example, an insider could issue a sequence of transactions to create a new customer account, add purchase transactions against the account, then add a credit to the account at the current date. The employee uses his insider knowledge and does this is in such a way that the account management application would generate a refund check to the customer. The fraud analyst could detect such a scheme if she had the ability to search across sessions for arbitrary patterns of activity. In general, an insider fraud control system should provide features that allow analysts to search across sessions using attributes of a session, such as the time of day a session started, as well as arbitrary patterns, such as a sequence of different transaction types.

Pattern Analysis and Reporting

Another technical functional requirement related to searching across sessions is the ability to generate reports based on pattern analysis. The previous section describes a hypothetical scenario in which an account management system might be tricked into generating an unwarranted refund check. An analyst might interactively search for such patterns, but a better option is to automatically monitor application activity and generate a report if such a sequence of events occurred. The combination of pattern analysis and automatic report or alert notification can be an informative set of tools that can help improve fraud detection without requiring analysts to run repetitive, interactive analysis operations.

The key functional requirements for an insider fraud control system include both business and technical requirements. Business requirements, such as industry-specific heuristics, usability, and configurable heuristics complement technical requirements; technical requirements include support for multiple platforms, real-time application activity monitoring, and the ability to search and analyze application activity data across sessions. In addition to these functional requirements, businesses should carefully assess a number of non-functional requirements.

Key Non-Functional Requirements

Non-functional requirements tend to address more global aspects of an application rather than an application's individual capabilities. Some of the most important non-functional requirements for insider fraud control applications include: scalability, security, and maintainability and vendor support. The following sections address important aspects to help ensure long-term viability.

Scalability

Scalability is the quality of an application to maintain acceptable levels of performance as the load on the system increases. Scalability can be achieved by adding servers as the load increases. In the case of insider fraud control, we need to consider the ability to scale as the volume of data grows and as the number of heuristics grows.

Figure 4.6: A scalable system will increase the amount of throughput in proportion to the increase in resources, such as servers. A linear increase in throughput with a linear increase in servers is often the best that can be expected.

Security

Of all the requirements we have discussed for an insider fraud control system, security is the most obvious. If the integrity and availability of such a system were compromised, the information it produced would be questionable at best and worthless at worst. In addition to basic security considerations, such as protecting the executable images that comprise the system, we need to ensure other processes and mechanisms are secure:

- Protecting log data as it is transferred into the system
- Maintaining correlated data
- Preventing tampering with heuristics
- Maintaining access controls on the system

In earlier chapters, we have discussed the limits of single-channel log data. Although log data from a single application is insufficient by itself to effectively detect insider fraud, log data from multiple systems can be a valuable source of data for an insider fraud control system. To protect the integrity of source data, access to the log data must be strictly controlled and any time the data is transferred into a fraud control system, it should be done over a secured channel. Encrypting communications between the fraud control system and data sources can effectively prevent eavesdropping and tampering with data in transit.

Once source data has been loaded, there will be a correlation process to integrate data from multiple systems. This process will generate derived data that may be slightly different from source data. For example, timestamps in log data may be normalized to a common time to eliminate differences due to variations in the time reported by different servers' clocks. The transformations that are applied to source data must be protected so that they are not tampered with.

Pattern recognition rules and other heuristics must also be protected against tampering. Clearly if the rules that are used to detect patterns of fraud were changed, the output of the system could be called into questions. Fraud control systems should have robust access controls on the heuristic repository. Changes to heuristics should be logged and reviewed to reduce the risk of unauthorized changes entering production. In the event an unauthorized change did reach production, it could be detected quickly and removed.

Access controls should be in place to protect all components that constitute a fraud control system:

- Executable images
- Link libraries
- Configuration files
- Documentation
- Database and data files

In addition to the technical controls incorporated by the fraud control system vendor, businesses should define and enforce their own procedures for monitoring how programs are updated, configurations changed, and log data generated by the fraud control system is reviewed.

Maintainability and Vendor Support

Fraud control systems, like other enterprise applications, will follow a life cycle that includes a series of changes to application code, documentation, and best practices. When evaluating fraud control systems, we consider how the system will be maintained without unduly disrupting production operations. For example, should the IT support group establish a test environment where upgrades and patches can be tested before applying them to production? If so, consult with the vendor on additional licensing charges if you were to run additional instances of the system in a test environment. Also review the vendor's policies on upgrades and patches. Specifically, what is the frequency of upgrades, are upgrades included in the base license fees, and how are critical patches distributed?

Businesses should also evaluate the vendor's ability to provide customization services. Fraud control systems are not the type of applications that lead to substantial markets for third-party support. These are not databases; they are specialized applications that require detailed knowledge to customize for specific business requirements.

Also consider the training services offered by the vendor. Training should be available for both systems administrators and for fraud prevention and security professionals that will use the system. Ideally, training should be available for the industry-specific heuristics that will be used in your environment. Training should include standard information that is provided to all customers, but be sure to have the vendor adapt the training material to your requirements.

The core non-functional requirements that one should consider are scalability, security, maintainability, and vendor support. Together with the functional requirements described earlier, these constitute the essential properties of a fraud control system that should be considered when evaluating these enterprise applications.

Support for Compliance Practices

The functional and non-functional requirements we have discussed are topics that we could describe to vendors and they could respond to. Ask a vendor how well their fraud control system scales, and they will probably show charts and graphs depicting reasonable or even impressive scalability. Ask about security controls in the application, and you will get a list of features designed to assure you that the integrity of the fraud control system is well protected. Ask about how the system will fit with your current compliance practices, and you probably won't get a polished response. As many consultants are fond of saying "It depends…"

When it comes to compliance practices and fraud control, we need to do a fair bit of self assessment and consider factors such as:

- How well the fraud control system will integrate with existing security policies and procedures
- Whether the fraud control system provides additional reporting and alert services that are not currently available
- How the fraud control system can support forensic investigation and incident response

A fraud control system can contribute significantly to improving how we implement security policies. As described in earlier chapters, single-channel monitoring is inherently limited. Multi-channel monitoring and real-time application activity monitoring can fill holes in our ability to capture and analyze data about events occurring in our enterprise right now.

Any enterprise application can generate reports, but data without context is useless. A fraud control system can provide reporting based on data consolidated and integrated from multiple sources. This task is not trivial and its difficulty should not be underestimated. It is likely that the reports and alerts available from a fraud control system will complement existing reporting services. Part of a vendor or application evaluation should be an assessment of how well the reports and alerts provided in the new application complement existing compliance reporting.

Effective forensic investigations are highly dependent on detailed data about an incident. A fraud control system that captures data in real-time from multiple systems, integrates that data, and filters it using general and industry-specific pattern recognition can be an invaluable tool. During the evaluation process, discuss with the vendor how the fraud control tool can be used for forensic investigations. Can historical data be "replayed" to help investigators understand the dynamics and the timing of particular events of the incident?

Enterprises considering fraud control systems probably have well-established compliance efforts in place; those systems can be supplemented and further supported by the additional features of a fraud control system.

Summary

Insider fraud and abuse is a fact of business. We can screen employees, implement robust security controls, and log application events and still fall victim to fraud and abuse. The consequences affect businesses financially and sometimes spill over to customers, patients, and clients who suffer a loss of privacy. Tools and practices for controlling fraud have matured, and today businesses have more options than ever before. Fraud control systems can implement multi-channel monitoring, support general as well as industry-specific heuristics for detecting fraud, and provide reporting and analysis tools to help identify potential fraud and abuse across the enterprise.

Download Additional Books from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this book to be informative, we encourage you to download more of our industry-leading technology books and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.