GURUCUL
PREDICTIVE SECURITY ANALYTICS

INSIDER ATTACKS

The Dangers and How to Prevent Them

WHITE PAPER

Introduction

The Exponential Growth in Data

Recent years and decades have seen the amount of data being generated growing exponentially. This phenomenon has led to the commonly used expression of Big Data becoming part of every day phraseology. Two statistics underline these trends succinctly. Big Data is a relatively recent phenomenon, but one that is set to expand due to the number of sources which are creating vast datasets rapidly increasing in number. This data has now grown in volume to thousands of terabytes, and in 2010, the CEO of Google, Eric Schmidt, asserted that the human race creates as much data in two days as it did in the entirety of 2003.As the geometric rise in information continues, cloud computing is becoming increasingly popular as a way to deal with collecting, collating and analyzing the vast amount of data now being produced by companies. It is already asserted that 80 percent of small businesses in the United States will utilize cloud computing as a central facet of their operations by the end of the decade.
One of the major sources of Big Data is business transactions. Almost all businesses are generating more and more information in the Big Data context, and much of this information is a cavalcade of sensitive data. It is predicted that if the US healthcare sector alone were to utilize Big Data creatively and effectively to drive efficiency and quality, then the sector could create more than $300 billion in value every year.
Thus, Big Data promises huge competitive advantages, and therefore it has become an invaluable asset for many companies. Unfortunately, along with the benefit of this data comes risks. Information is increasingly available to larger numbers of people, with an expanding user base of employees, business partners, suppliers and customers all requiring access to various types of data. IT infrastructures have evolved to deal with this issue, becoming more accessible and distributed, and security issues arise from this situation.
Government laws have evolved to help protect confidentiality, with the United Kingdom, for example, passing the Data Protection Act of 1998. But in the climate of Big Data and complex computing networks that exists, there will always be the threat of insider attacks from people within an organization with a vested interest or malicious intent.

As businesses increasingly require and operate more access points, so the potential for data theft and security issues increases as well. Not only are companies and organizations faced with practical considerations but government has also put in place stringent regulatory requirements to which businesses must adhere.

33 percent of information security attacks actually originate from internal employees, with a further 28 percent emanating from ex-employees and partners of the company.

The Looming Threat of Insider Attacks

The threat of insider attacks is nothing new; indeed, organizations have spent decades attempting to deal with this very issue. In a direct reaction to such potential problems, IT companies have developed a range of methods to protect themselves against intrusion and most of these are familiar to the average computer user. Thus, such concepts as firewalls, anti-virus software and biometric protection are familiar to virtually all of us.

However, much though such technology provides a valuable line of defence for businesses, it can only be viewed as a front line. While these methods are generally good at providing unauthorized access, they are not always much of a protection against insider attacks.

According to PricewaterhouseCoopers' "The Global State of Information Security 2005", 33 percent of information security attacks actually originate from internal employees, with a further 28 percent emanating from ex-employees and partners of the company. Even a basic grasp of mathematics should indicate that this means that the majority of security threats actually come from people who businesses would generally believe that they can trust.

Unfortunately, it is impossible given the following information to simply trust one's internal employees and customers. Insider attacks are a serious threat, and they simply must be treated as such. The greatest vulnerabilities experienced by any businesses are felt by those who simply underestimate the potential damages that can be caused by employees and other internal sources. Businesses have a tendency to prioritise protection against issues such as DDoS attacks, financial fraud and viruses, but it is foolish in the extreme to neglect insider attacks.

While external threats traditionally receive more media attention, the notion of insider attacks has also gained some traction recently. Most notably, the revelations which were highly publicized by former National Security Agency employee Edward Snowden gave an example of how insiders can penetrate internal systems and render an organization vulnerable to attack.

Of course, in the case of Snowden many people wholeheartedly supported his actions, but the incident still underlines the extent to which insider attacks can compromise an organization's operations.

There have been a huge amount of prominent insider attacks reported in recent years, and the commercial and financial damage caused by these incidents has been pretty hefty. For example, in June, 2006, the back-office processing and customer support firm HSBC Electronic Data Processing reported that an employee had accessed customer debit card information and used it to defraud twenty UK customers of $425,000.

The Privacy Rights Clearinghouse, a Californian nonprofit corporation focused on consumer information and consumer advocacy, has found that literally hundreds of internal data breaches have taken place over the last decade. As early as 2009, the world's largest software company had warned that the number of insider security attacks from disgruntled workers would increase in the precarious financial climate. Microsoft's Doug Leland noted that "with 1.5 million predicted job losses in the US alone, there's an increased risk and exposure to [insider] attacks".

Some of the most notable **insider attacks** that have occurred in recent years includes:

- The UBS PainWebber case which cost the bank $3.1 million, and resulted in 97 months in prison for Roger Duronio.
- The compromising of 200,000 bank accounts by a call center in Pune, India. A company involved in offshoring failed to handle sensitive data appropriately and inadvertently allowed access to contractors.
- Terry Childs, a system administrator for the city of San Francisco, changed passwords to the FiberWAN system that carried the majority of network traffic for the San Francisco city government. The system was locked out for 12 days and cost nearly $1 million to repair. Childs was sentenced to four year in prison.
- One of the most high profile insider attacks involved Bradley Manning leaking material from the Department of Defense's Secret Internet Protocol Router Network and passing it to the activist group Wikileaks.

Painting by: Leonardo Ruggieri

Some of the most notable **insider attacks** that have occurred in recent years includes:

- The UBS PainWebber case which cost the bank $3.1 million, and resulted in 97 months in prison for Roger Duronio.
- The compromising of 200,000 bank accounts by a call center in Pune, India. A company involved in offshoring failed to handle sensitive data appropriately and inadvertently allowed access to contractors.
- Terry Childs, a system administrator for the city of San Francisco, changed passwords to the FiberWAN system that carried the majority of network traffic for the San Francisco city government. The system was locked out for 12 days and cost nearly $1 million to repair. Childs was sentenced to four year in prison.
- One of the most high profile insider attacks involved Bradley Manning leaking material from the Department of Defense's Secret Internet Protocol Router Network and passing it to the activist group Wikileaks.

The Potential Costs of Insider Attacks

One should not underestimate the potential cost of malicious insider attacks. A recent report produced by the IT security research firm Ponemon concluded that the average insider attack can take around 65 days to contain satisfactorily, which is significantly longer than the average external cyber attack.

Additionally, the organization estimated that resolving an insider attack will cost around $1.5 million, which represents a 33 percent increase from the estimated average cost in the organization's previous report.

incidents which actually cause financial losses to enterprises involve insiders, but that 60 percent of those are unintentional. Either way, internal information is the cause of such issues, rather than external attacks.

Given that internal attacks are carried out by people who are essentially trusted, the attacker often has the privilege of pretty much unfettered access to their particular target. Very specific and important information can be easily isolated, and the ability to exploit established entry points and obscure vulnerabilities will always be likely. Inside attacks are more difficult to detect, harder to contain, and potentially more damaging than external attacks, yet they remain relatively unpublicized compared to such phenomena as viruses and hacking.

The Association of Certified Fraud Examiners (ACFE) found in its "2006 ACFE Report to the Nation on Occupational Fraud and Abuse" that the majority of cases of general fraud are instigated by tips provided by existing employees, or simply by accident. In accordance with this notion, the Gartner Group estimates that 70 percent of security

While there is an immediate focus on the amount of money that insider attacks cost, there could be a raft of other consequences as well. It is possible that a company's competitive position could significantly suffer if intellectual property or trade secrets are stolen and then distributed among competitors. Although businesses may have some legal recourse under these circumstances, there is no court decision which can prevent a competing business from gaining an advantage in the marketplace if they haven't committed a criminal offence. Attacks can also be physically designed to damage the reputation of a company; thus, insider attacks carry business, competitive and commercial consequences as well as mere financial penalties.

Given all of the factors discussed previously, it is obvious that addressing the threat of insider attacks is extremely important to any business.

Protecting Your Company Against Insider Attacks

Thankfully, you are not completely alone when dealing with the threat of insider attacks. Gurucul has developed an intuitive and intelligent system, which it dubs Actionable Risk Intelligence, which has the ability to detect risky and suspect behaviors as or before they occur.

The sophisticated algorithms included within Gurucul's software are actually self-learning, and protect you against the potential horrors of insider attacks by consolidating identity profiles with machine data and providing alerts from defense-in-depth security solutions, enabling you to create 360° context aware timeline visualizations.

This value is further extended by the software creating behavior baselines and peer group analyses, enabling your business to prevent, detect and mediate against any unknown anomalies within your internal systems.

Actionable Risk Intelligence continually monitors your internal systems and seeks out dangerous threat patterns, and assesses them as they evolve over time; profiling the lifecycle of events, as opposed to simply the perpetrator or suspected attacker. The internal incident response system and integration which Gurucul provides also ensures that any suspicious activity is elevated extremely quickly.

These are only some of the benefits of the functionality-rich portfolio of features which have been packed into this software, and in the context of dangerous insider attacks discussed in this white paper, coping without some software protection against this threat is quite simply extremely unwise.

About Gurucul

Gurucul is dedicated to transforming the cyber security landscape using machine learning, intelligence-driven, big data security analytics. Using identity as a threat surface, Gurucul provides Actionable Risk Intelligence™ to protect against targeted attacks and under-the-radar cyber campaigns. Gurucul is able to proactively detect, prevent and deter advanced insider threats, fraud, and external threats to system accounts and devices using sophisticated self-learning, advanced behavior and anomaly detection algorithms.

Gurucul is backed by a strong advisory board comprising of fortune 500 CISOs, world renowned experts in government intelligence and cyber security. The company was founded by seasoned entrepreneurs with a proven track record of introducing industry changing enterprise security solutions. Their mission is to deliver rapid results to any organization that desires to protect its intellectual property, regulated information, and brand reputation.

GURUCUL | 5959 W. CENTURY BLVD. SUITE 1111. LOS ANGELES. CA 90045 | 213.373.4878 | INFO@GURUCUL.COM | WWW.GURUCUL.COM