

Compliance Monitor

The monthly briefing service for compliance specialists

Look within

Financial institutions face a growing menace of corrupt insiders. What steps can financial crime compliance take to foil the enemy within? Brian Contos, chief security officer, Arcsight Inc, has a suggestion.

Late last year, Callum McCarthy, FSA chairman, warned of the insider threat. Staff have been blackmailed and bribed to supply confidential information and there is nothing new in unhappy or demotivated employees who seek to inflict damage on the (perceived) source of their grievance: their employer. In some cases thieves might steal a bank account number or address; in others it may be an entire 'wallet' that contains financial, health and other personal data. These details are sold on to criminal gangs with the risk that they will be auctioned to the highest bidder on an underground version of eBay.

Worryingly, for everyone concerned with protecting corporate security, police say insider threats have grown over the past 18 months – and have worsened considerably recently. In a report last year the National Hi-Tech Crime Unit (NHTCU) noted that acts of sabotage and data theft were most often committed internally – the culprit was an insider in over two-thirds of data theft cases.

In true chameleon fashion, criminals have identified the corporate weak spot. The perimeter has become increasingly resilient to attacks with firewalls, virtual private networks (VPNs), two-factor authentication, operating systems and other devices updated nowadays on an automatic basis. There are far more loopholes on the inside: from doors left open through to lax vetting procedures, easily accessible passwords and the outdated

legacy systems fixed together by 'sticky plasters' that sit at the heart of most financial institutions. From a criminal's perspective, why focus on battering down a steel door when they could go round the back and smash a glass window?

It can be as easy as plugging in a USB key, sending an Instant Messenger attachment or using Internet mail to download a customer's account details and cause havoc for a financial services provider. Worryingly, it does not require extensive IT expertise or knowledge of hacking systems. Traditional

mechanisms such as strong authentication, identification and authorisation access points can pose little deterrent if the activity is conducted under the guise of doing one's job.

Many forward-thinking organisations put in place preventive measures that focus on people, process, technology and information; these include access controls,

separation of duties, and defence-in-depth solutions, which employ multiple layers of security. For example, protection around a critical server may include firewalls, intrusion detection, anti-malware solutions and encryption as well as monitoring of its logs, strict access controls, a 'hardened' operating system and defined policies and procedures surrounding its use. However, prevention does not always scale well, and unless detection methods are also used, the most subtle and the most advanced attacks will go unnoticed.

A significant part of the problem is the way that financial services institutions detect insider threats. Currently, about 75% of checks are manual according to

Many forward-thinking organisations put in place preventive measures that focus on people, process, technology and information; these include access controls, separation of duties, and defence-in-depth solutions, which employ multiple layers of security.

the 2005 Insider Threat Study published by the US Secret Service and Carnegie Mellon University. Yet as companies that once relied on manual detection systems for external threats know all too well, such systems are inadequate at identifying security breaches, often because there is simply too much security information to wade through with the result that many attacks are likely to go undetected.

To put this in a real world perspective, a business traveller could log into his company's network via a VPN from Sweden. At the same time, a criminal could be activating his desktop PC password back in the UK headquarters. One of these attempts has to be a criminal act, since the employee cannot be in two places at once. But such a threat might not be detected in a manual environment where the most common analysis method is diving into disparate device logs, akin to looking for a needle in a haystack.

In a bid to overcome this problem the last couple of years has witnessed a trend towards a holistic view of corporate security with convergence of network monitoring, physical security, communications security and IT security. This trend is also evident in the emergence of new job titles such as chief risk officer. At the same time there is evidence of greater collaboration across the industry: the FSA noted in its February paper on management of fraud risk that both APACS and CIFAS are working on initiatives that will allow members to share information on staff fraud cases.

In the meantime, organisations could address one of the main barriers to detecting insider threats

simply by automating the way in which threats of this nature are detected, as has been done at the perimeter level. Known as 'security information management', this has become an increasingly important area of best practice in securing a company's network. Most companies are so inundated with security information from each point security device that they simply do not have the resources to correlate the information, make sense of it and identify any deviant activity.

Unfortunately, there is no silver bullet that can put an end to insider threat. Dissatisfied or mercenary employees and criminals will always seek to take advantage of security holes. This is why real-time correlation is central to reducing and managing risk. Individual events may pose no obvious threat, yet when correlated, innocuous network occurrences may appear as malicious attacks.

Financial crime compliance and corporate security officers need to continually weigh up threats in the context of the whole organisation, not just each subsection, such as the perimeter or physical security. This is where security information management systems (otherwise known as enterprise security management systems) can play a lead role – alongside best practice policies, procedures, documentation and training – in creating a single, comprehensive view of the organisation's IT risk, and employing advanced correlation and pattern discovery techniques to match apparently unconnected events.

Brian Contos, CISSP, Chief Security Officer, ArcSight Inc.

ArcSight, a leader in Enterprise Security Management, provides solutions that serve as the mission control center for real-time threat management, compliance reporting and automated network response. By comprehensively collecting, analyzing and managing security data, ArcSight solutions centrally manage and mitigate information risk for security, insider threat and compliance. ArcSight's customer base includes leading global enterprises, government agencies and MSSPs.

ArcSight 