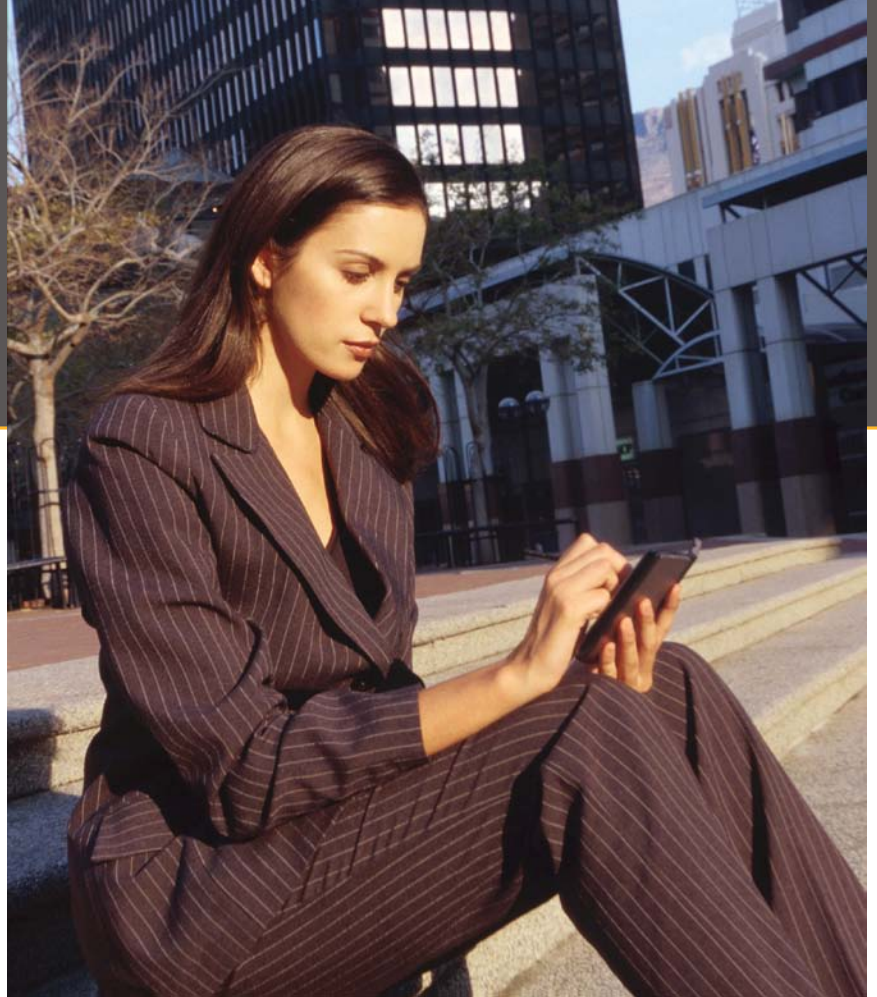




# Protecting Sensitive Data from the Inside



For much of the recent past, attention has been focused on preventing attacks from the “outside”. However, employees, vendors, partners and other trusted insiders have become an increasingly significant threat to corporate networks and information assets. They have access to a vast array of business critical and confidential data, leaving companies and individuals vulnerable to a variety of deliberate and accidental exposures.

## Prevention

One of the first steps to protecting against security threats from inside your organization is to review your stated policies and procedures. Equally important is implementing and observing best practices in terms of people management. Prospective employees should be properly screened and background checks should be conducted as condition of employment and a culture of security awareness should be cultivated through ongoing training.

## Leverage Technology

An organization needs well-established and fully tested access controls, system baselines, content filtering and monitoring. It is important to conduct periodic self audits and to confirm that logging and alerting provides sufficient detail to identify an intrusion or repeated failed attempts at access.



*The insider threat is a complex problem which encompasses your entire organization and necessitates a coordinated and integrated effort from all parties.*

Logs should be aggregated and reviewed daily, exceptions should be documented, suspicious events investigated and all logs archived for a period of time consistent with business and legal requirements. Every unexplained deviation should be documented as an event until a definitive justification is found or it merits initiating the Incident Response (IR) Plan.

## Responding

When an incident occurs, the most important thing is a well defined, executable IR Plan that has been developed with input from multiple business units. Validating your response plan is the key to responding quickly, logically and appropriately so you can resume normal operations. You should be prepared to respond swiftly to mitigate the incident, notify legal, law enforcement and all affected individuals. As you review your organization’s Incident Response Plan, consider the

applicability of the following generally accepted guidelines.

- Control information disseminated to the public during a security incident. Consider enlisting the service of a public relations firm.
- Establish a central point of contact.
- Notify legal counsel as dictated by your plan sooner rather than later.
- Establish a chain-of-custody procedure that tracks who has been involved in handling any evidence.
- Do not contact suspected perpetrators.
- Minimize changes to your systems until they are forensically imaged.
- Ensure all logging capabilities are enabled and not set to overwrite.

## Getting Started

As an experienced business consulting and security provider, SARCOM can take the role that best meets your requirements. Call your SARCOM Account Executive today, before your security threats become a devastating reality.