GOING "ALL IN" ON DEFENDING AGAINST INSIDER THREATS

Industry Best Practices

Data Sheet: Industry Perspectives—Federal Government

Government agencies have always been exceedingly concerned about security—but that concern ramped up significantly in the wake of the Edward Snowden and Bradley Manning scandals.

As part of the galvanized response to these two incidents, agencies took a more serious look at fighting and preventing insider threats. These threats can be difficult to discover and can often do far more damage than their external threat counterparts.

Internal threats can take many forms. They can be malicious, as evidenced by the Snowden and Manning cases. They can also be the result of carelessness; after all, it's very easy for an overworked administrator to misplace a USB drive, leave a laptop unattended, or forget someone's access from a major Fileshare. These factors can make internal threats very hard to detect and predict.

The existence of various threat levels further complicates matters. Some threats might be substantial, and have the ability to cause massive havoc and damage. Others might be less severe, but still cause problems—system downtime, for example.

Regardless of the threat level, a systematic plan to combat insider threats is a must. This complete and consistent plan must account for everyone and anything that has access to valuable information, including anyone who has access to your systems -- not just employees, software, or an unauthorized device accessing the network.

A Complete Plan to Fight Insider Threats

Securing against insider threats should not be planned or implemented in a piecemeal fashion. To do this right, agencies must go "all in" and develop a holistic plan and strategy that considers everything (and everyone) that touches the network and has access to valuable information—including people and technology.

The Department of Homeland Security separates the fight against insider threats into four categories: Trust, Behavior, Credentials, and Privileges:

REVIEW OF THE PHASE 2 CAPABILITIES

TRUST	BEHAVIOR	CREDENTIALS	PRIVILEGES
			
• People • Suitability • Clearance • Entry on Duty	• Training • Monitoring • Reporting	• Credential Type • Assurance Level • Account Linking	• Roles • Security Groups • Attributes

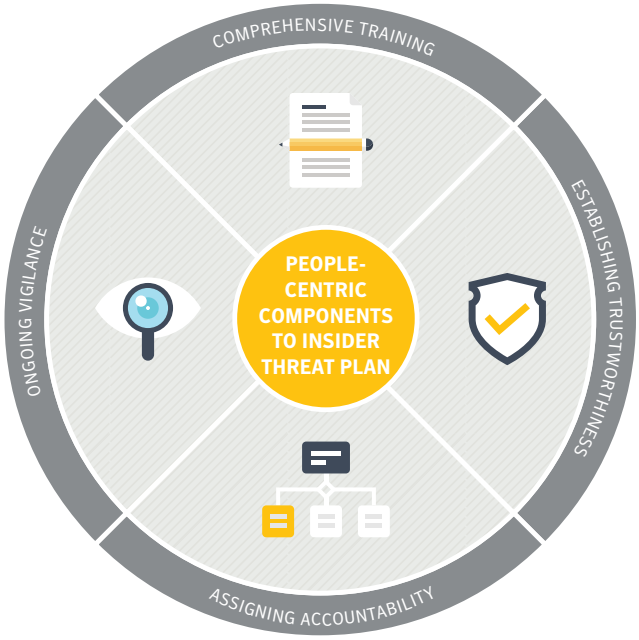
Symantec™

Successfully combatting insider threats involves creating a strategy touching on each of these categories, and that requires a focus on both people and technology. As such, plans against insider threats must encompass a personal and procedural approach. The personal approach involves working with people to make sure they are empowered to fight threats and trained to prevent accidental information leaks. The procedural approach incorporates the development of processes and policies that take technology into account. Let's take a look at both.

The Personal Approach: Employee Security

There are four essential people-centric components to every insider threat plan:

Comprehensive training should serve as the cornerstone of any insider threat management strategy. All employees, both new and old—even those peripherally involved in the management of secure information—should undergo comprehensive training procedures. Training should focus on agency-specific parameters and include details on the latest government security initiatives and policies.



Establishing trustworthiness can ensure the empowerment of IT administrators while protecting the network. The old Russian proverb that advises to "trust, but verify," can be applied to IT managers who must vet prospective and current employees. Managers must check their credentials, ensure they are properly trained, and more. These processes can be particularly instrumental in protecting against malicious threats, but can also help mitigate the potential for carelessness, as the need for continued awareness will be impressed upon employees.

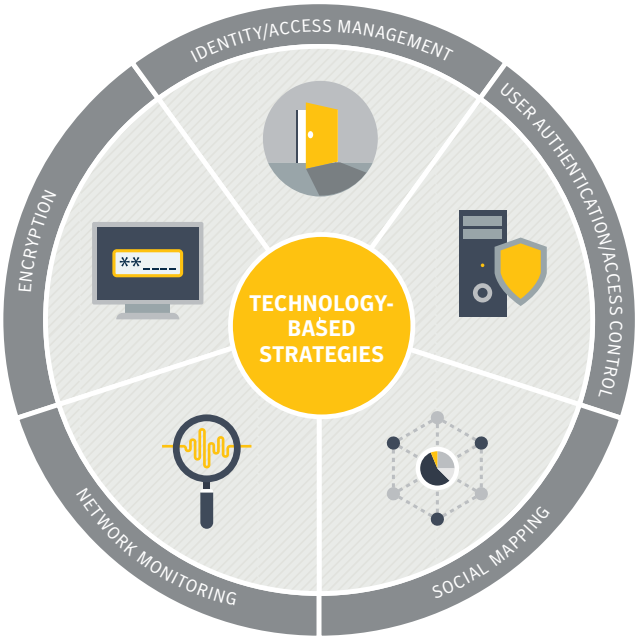
Assigning accountability involves treating all users as assets. Each user's role and responsibilities should be clearly defined, so that there is a distinct understanding of their authorization level and credentials. Accountability can help track potential problems back to individual users, while helping everyone understand what they do and do not have access to. Everyone's motto should be "manage the user, mitigate the threat."

Ongoing vigilance is necessary to ensure that insider threats are kept to a minimum. Employees must be continually on the lookout for potential warning signs, and agencies must invest in the proper tools and technologies to help them in this endeavor.

Symantec™

The Procedural Approach: Technology Security

Agencies should include five technology-based strategies to complement their employee-centric approaches:



Proper **Identity and Access management** is absolutely essential to any security initiative. Agencies must account for all of the data they possess. Too often, however, they stockpile data that's old and no longer valuable. This practice can pose a significant security risk; it often exists undetected, and agencies may not realize if an unauthorized user has gained access to it. While the data may still exist online, no longer serving a purpose, it remains available for insiders to exploit (Bradley Manning, for example, gained access to data that should have previously been archived or deleted).

To protect against this, agencies must employ solutions and strategies that support proper data hygiene and security practices. Doing so will enable the identification and safeguarding of data that is viable and relevant, while eschewing information that is no longer usable.

Safeguarding viable and relevant data involves implementing stringent **user authentication and access control** principles. Excessive or unauthorized access permissions are one of the main culprits behind insider threats. Often, too many users are granted authorization to databases they do not need to access, or employees have multiple permissions for accessing data. Both approaches can pose extreme risk.

Agencies must streamline user authentication and access control procedures as much as possible. Only users with a "need to know" should be granted access to secure databases, and access should be restricted to a minimal number of individuals. Furthermore, human assets and identities must be continuously and closely monitored to ensure that unauthorized users are not gaining access to critical data.

Social mapping can play a key role in thwarting successful insider threats by monitoring and baselining user behaviors. IT social mapping "learns" how users behave on the network while interacting with applications and data. Analyzing this data will help organizations identify anomalous user activity denoting potentially risky or unauthorized behavior. Social mapping can identify users who might be attempting to steal sensitive information. It can be useful in showing various outliers that could pose a threat to the agency, i.e., a user who has access to an inordinate amount of proprietary data.

Network monitoring is another important component in battling potential insider threats and can help prevent critical issues from arising. Unusual user behavior can be flagged and addressed immediately through network monitoring. Unauthorized devices pinging the network can also be identified, which can support agencies' efforts at "bring your own device" management. Further, everything is automated, which takes a large burden off IT administrators.

Finally, agencies should implement **encryption** procedures to protect sensitive data. Endpoint, files, folders, and emails may all be encrypted. Also, agencies should take care to encrypt sensitive data that might be moved to and stored on removable devices, such as USB drives. Individual and group key management, automated policy controls, and compliance-based reporting should may all be implemented in conjunction with encryption protocols to form a complete and airtight security plan.

Symantec

The Symantec Approach: A Complete Solution

Symantec offers a wide array of solutions designed to help agencies prepare for–and avert–insider threats. Our security portfolio includes tools like:

Risk Management and Compliance:

Symantec Data Insight, which helps organizations improve unstructured data governance through actionable intelligence and by providing insight into data ownership, usage, and access controls.

Symantec Data Loss Prevention, which identifies confidential data location and usage and protects it from loss and theft.

Symantec Control Compliance Suite, which delivers business-aware security and risk visibility so that customers are effectively able to align priorities across security, IT operations, and compliance.

Symantec Data Center Security, which features security hardening and monitoring for on-premise data centers and public and private clouds.

Identity and Access Management:

Symantec Validation and ID Protection Service, which enables agencies to secure access to networks and applications while preventing access by malicious unauthorized attackers.

Symantec Identity: Access Manager, which helps fill the gap in the cloud where a traditional enterprise perimeter doesn't exist. A next-generation access control platform that integrates Single Sign-On (SSO) with strong authentication, access control and user management, Symantec Identity Access Manager offers users and administrators control, convenience and compliance for Web- and cloud-based applications.

Endpoint Security and Encryption:

Symantec Endpoint Protection, which enables for the proactive identification of at-risk files and stoppage of zero-day threats without sacrificing performance.

Symantec Endpoint Encryption, which provides organizations with strong full-disk and removable media encryption with the ability to integrate with Symantec Data Loss Prevention for an even stronger security solution.

More Information

For more information about all Symantec security products, visit www.symantec.com.
To learn more about security, visit http://www.symantec.com/security_response/, or visit Symantec's security community.
To speak with a Product Specialist in the U.S. Call toll-free 1 (800) 745-6054

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.comor connect with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec