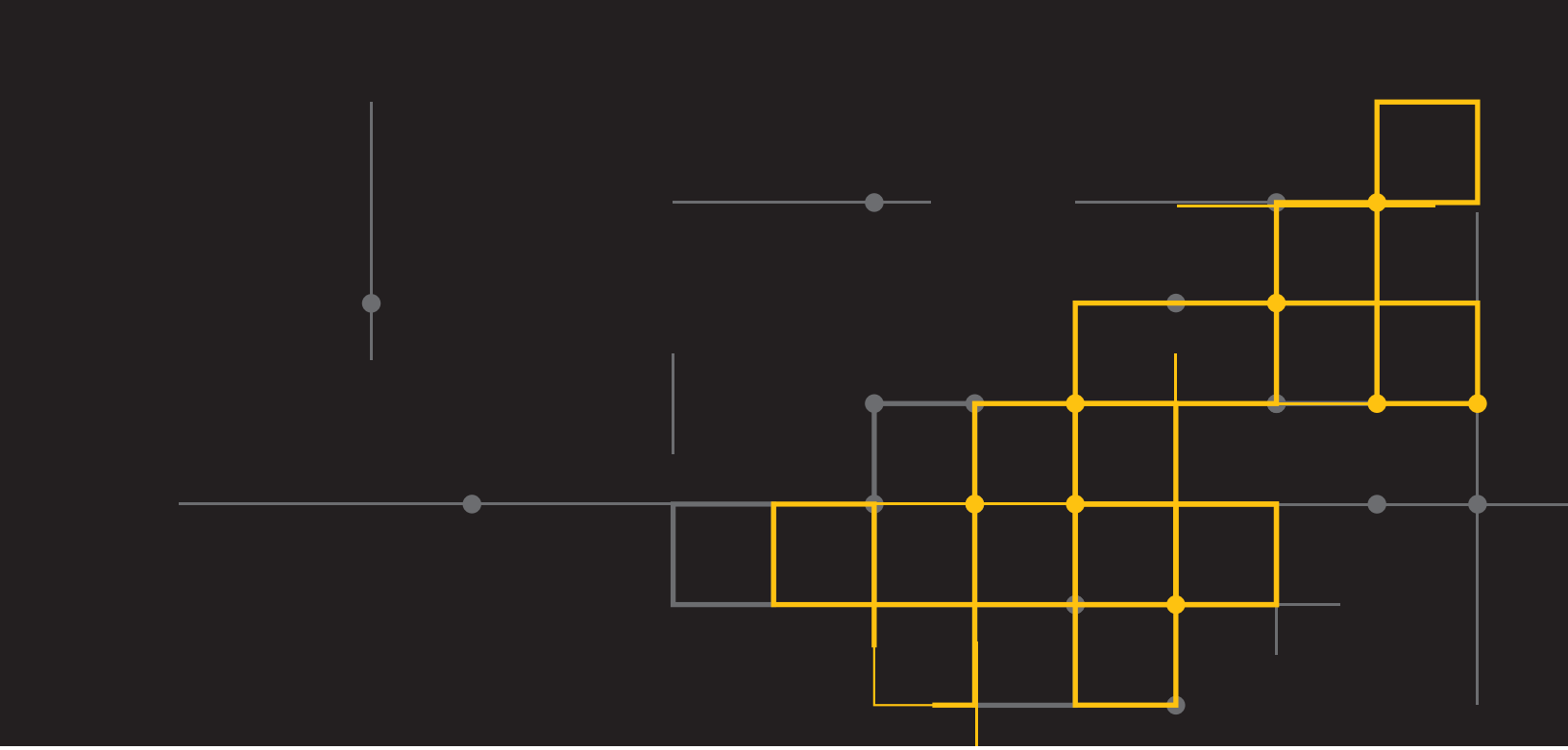

Implementing an Effective Insider Threat Program

White Paper | May 2017

Symantec

Government agencies need more than security tools and solutions to defend against today's constantly evolving cyber threat landscape. A cybersecurity culture must exist within all levels of an organization – starting at the top with C-level executives and flowing all the way down to the individual employee. While many agencies focus on preventing inbound attacks from occurring, some are behind on tracking what type of information is leaving the agency and how. To successfully conduct assigned missions and serve the American public, the government must have strong security controls for both inbound and outbound data to enhance an agency's cybersecurity posture.

The Risk of an Insider Threat

The National Counterintelligence and Security Center describes an insider threat as an incident that occurs when a person with authorized access to U.S. government personnel, facilities, information, equipment, networks and systems, uses those resources to harm the security of the United States. All it takes is for one negligent worker, whether intended or not, to expose an agency or department to a malicious breach. With a click of the mouse, an insider can release an enormous amount of sensitive data to cyber criminals and in an instant, permanent damage is done to victims and agency reputation.

Consider Harold Thomas Martin, III, the former National Security Agency private contractor who collected approximately 50 TB of secret and top-secret information and stored it at his home. Over two decades, Martin used his credentials to collect and store numerous classified documents from the NSA, USCYBERCOM, the National Reconnaissance Office and the Central Intelligence Agency. Even though he held a security clearance for 28 years and a Top-Secret security clearance for 13 years, served in the U.S. Navy, and, worked as a government contractor for the Department of Defense and within the U.S. Intelligence Community, this formerly trusted insider's actions put the nation's security at risk.

The Cost of Insider Threats

Although the monetary cost of a data breach to an organization is high—reportedly more than $7 million—the cost to the mission is even more significant. An agency must consider the value of the systems or data compromised in addition to the cost of legal and compliance penalties. A breach can tarnish a reputation and make it difficult to recruit future employees, resulting in a loss of faith in the agency's ability to successfully carry out its mission. Breaches often cause political action involving lengthy congressional hearings and taking time and resources away from the agency's mission – just ask the Office of Personnel Management. Ultimately, a breach as a result of an insider threat can cause exposure to some of the country's most valuable assets—personally identifiable, proprietary, sensitive or classified information—putting the mission at risk and opening up a world of intelligence to adversaries.

Some data breaches happen because of a careless mistake, while other attacks are carried out with malicious intent. Regardless of how a data breach occurs, no agency wants to deal with the repercussions of not having a solid insider threat program in place. It is the government's job to put policy and controls in place to ensure that cyber threats, including insider threats, are mitigated as soon as possible.

Cybersecurity Policies – A Good Start, But Not Enough

In 2011, following the massive release of classified information through WikiLeaks, President Obama issued an executive order establishing the National Insider Threat Task Force. The organization's mission is to develop a government-wide insider threat program that can prevent, deter, detect and mitigate compromises of classified information by malicious insiders who may represent a threat to national security. A year later, the National Insider Threat Policy was implemented to promote the development of insider threat programs within departments and agencies.

Given that the Office of Management and Budget's annual report to Congress on federal cyber performance indicates that federal agencies experienced 30,899 "cyber incidents" in fiscal 2016 that caused the "compromise of information or system functionality," more needs to be done. Cybersecurity policies are certainly an important component of formulating a comprehensive insider threat program, but they are only as strong as the next end user. Policies alone cannot prevent breaches and have no impact on malicious end users who are intent on doing damage.

Building an Insider Threat Program

There is no "easy button" for solving the insider threat problem, but fortunately, senior agency leaders do have a tool in their cyber toolbox to help establish better control over their cybersecurity program and manage cyber risk – the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). This tool was developed through collaborative engagement with the private sector and provides a common structure for managing cybersecurity risk that is flexible and adaptable, and can be used by all government organizations, whether they already have a cybersecurity program or are just establishing one. It is not meant to replace any existing security programs or practices, but serves as a supplement.

Government agencies have been directed to use the CSF to facilitate the measurement, mitigation and reduction of risk. Taking that a step further, Thomas Bossert, an adviser to President Trump on homeland security and counterterrorism, recently said that "the new administration will require agencies and departments to abide by the framework developed by the National Institute of Standards and Technology (NIST) and report back to the White House on their adoption and implementation of the cybersecurity recommendations."

In addition to using this government guidance to build an effective insider threat program, agencies also need to incorporate technology to help enforce, protect, manage and extend cybersecurity policies and guidance.

The most effective way to develop an insider threat program is through a multi-layered approach based on vendor agnostic cybersecurity best practices and proven technology. This is the only way to secure government data wherever it resides or travels, in a way that will enable agencies and departments to evolve their cybersecurity protection strategy with constantly changing insider threats.

By using the CSF as a baseline and incorporating an end-to-end technology capability, government stakeholders can develop a strategy that will safeguard the safety and reputation of the agency; discover sensitive data wherever it resides and identify endpoints at risk; monitor the ways sensitive data can be used and flag abnormal behavior; and, utilize the most efficient and unobtrusive methods possible so the government mission is not negatively impacted.

The goals of the CSF include directing organizations to perform the following five core functions concurrently and continuously to address risk within a dynamic operational culture. The federal government must **IDENTIFY** and locate data that needs to be protected, whether at rest, in use or in transit on the network, in the cloud, on mobile devices or traversing the Internet. Agencies can **PROTECT** their data, **DETECT** attempts to corrupt or steal data, **RESPOND** to cyber-attacks or insider threats and **RECOVER** from the attack, while using the lessons learned to adjust security policies and fill in any existing gaps. See Figure 1 below.

Figure 1: NIST CSF-Insider Threat

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management • Asset Management • Governance	**Prevent Incursions** • Access Control • Awareness and Training • Data Security • Information Protection Processes & Procedures	**Detect Infections** • Anomalies and Events • Security Continuous Monitoring • Detection Processes	**Contain Infestation** • Analysis • Mitigation • Improvements	**Return to Normal** • Recovery Planning
• IT Management Suite • Data Loss Prevention • Data Center Security	• Data Center Security • Data Loss Prevention • VIP/SAM • Control Compliance Suite • Norton Secure Login • Proxy • Website Security • CASB • Cloud Data Protection	• Data Center Security • Cybersecurity Simulation • Managed Security Service • Security Analytics • Proxy • Website Security • CASB	• Incident Response Service • Data Loss Prevention • Security Analytics	• Incident Response Service

Deploying Technology

Government agencies achieve the five key goals – identify, protect, detect, respond and recover – by using the CSF as a guide and by deploying technology that addresses the following:

- **Identify the Appropriate Data Owners**. Find out who is using the data and who would be impacted if the data was modified. Use technology to identify system users and prioritize what they think is the most critical data. Work with these data owners to further identify additional priority data types to reduce risk.

- **Locate Where the Sensitive Data Resides and Tag It**. Consider data at rest, data in use, data in motion, archived data and encrypted data. Also consider standard locations including network devices, storage, databases, file servers, web portals and other applications, laptops, email servers and PST files. Think about other locations such as mobile devices, printers, scanners, fax machines, copiers, file sharing apps like Dropbox or Evernote, any type of removable devices like USB drives, CD/DVDs, paper copies, instant messaging, "free" webmail services or FTP sites. Look anywhere movement or spillage of data occurs, and once it has been located, develop a system that will tag it.

- **Monitor and Learn How Sensitive Data is Generated and Used**. How is sensitive data generated by the agency's workforce and are there multiple instances of it? Determine how many channels and platforms are available where something could go wrong that could impact sensitive data. The larger the infrastructure, number of employees, geographic locations and types of platforms used, the more issues are possible.

- **Implement Automatic "Real-Time" Methods to Enforce Security Policies**. Once an agency implements its data security policies, risks will be reduced over time. The goal is to get to the prevention stage so that when sensitive data starts moving in a way that violates organizational policies, it's immediately flagged and remediation actions are taken against it. Once an agency understands where its data is stored and how its data assets are used across the agency, it can identify broken business processes and high-risk users, clean up misplaced data and provide specialized training. Automated e-mail and onscreen pop-up notifications can educate users about data loss policies, cutting down on the number of repeat offenses. Lastly, users can be prevented from accidentally or maliciously leaking information by quarantining, encrypting and blocking inappropriate outbound communications.

- **Educate Systems Administrators and End Users**. Go over policies regarding sensitive data security and elevated rights while stressing that this type of access requires great responsibility. Systems administrators may not realize that policies exist for certain data types, so maintaining a clear and consistent line of communication and education is important.

- **De-escalate Excessive Systems Administrator Privileges**. Most systems administrators don't require administrator rights beyond what they need to complete their assigned job functions. Separation of duties is a cybersecurity best practice for thwarting the systems administrator "insider threat."

- **Wrap Additional Security Around Sensitive Data**. The best incident response is to thwart the incident in the first place, long before it becomes an incident. As such, it is important to regularly review file permissions. A user or group of users may have permission to use certain data, but once they are moved off of that mission, give access only to what they need and have management constantly reviewing those privileges. Also, consider using additional encryption for sensitive data as part of a defense in-depth posture.

- **Halt Data Leaks Before Spillage Occurs**. If an incident can be stopped dead in its tracks, the damage and post-incident cleanup can be minimized. The best way to reduce time and resources required to respond to an incident is through response automation. By automating the process, the incident can be routed to the right responder in a prioritized fashion so that the most severe event can be prioritized first. With the correct information, a responder can provide the appropriate action and kill an incident before it can inflict more damage. Finally, metrics can prove to executives and auditors that the right response was taken.

A key benefit of this multilayered approach is that it works at all cybersecurity maturity levels. This should start with an assessment of an agency's cybersecurity maturity to identify current gaps

and risk areas, prioritize them, and begin to fill in the gaps over time. Using the CSF's five functions, categories and subcategories, agencies can identify the gaps in their protection strategy, and work to find ways to fill them. While employees are the life-blood of agencies, they also pose the biggest risk to data and operations. It is critical for agencies to take the insider threat seriously, focusing on enforcing the CSF through the implementation of a robust cybersecurity solution suite in a multi-layered approach.

Why Symantec?

Symantec is the only company who can provide a comprehensive insider threat capability that prevents, detects and reports on unauthorized attempts to exfiltrate data from the internal network, mobile devices and the cloud. As highlighted below, our solutions provide that multi-layered approach and align perfectly with the NIST CSF, enabling agencies to have confidence that their insider threat program is, and will remain effective.

NIST Function	{TOPIC} Protection Requirement	Symantec Solution
IDENTIFY	Automated solution to discover, classify and tag all sensitive information on the enterprise network, in the cloud and on mobile devices.	Data Loss Prevention
PROTECT	Password-free or multi-factor authentication system.	Validation and Identity Protection
	Secure single sign-on to cloud and web applications that leverages multiple existing identity services to authenticate.	VIP Access Manager
	Cloud-based identity service that provides identity proofing, credential issuance, credential validation, attribute validation, and single sign-on services.	Norton Secure Login
	Prevent data from exfiltration from removable storage devices, mobile devices, data center servers, cloud environments and PC endpoints.	Data Loss Prevention
	A cloud-based service that enables organizations to issue, renew and revoke digital certificates that can be used to power strong authentication, encryption and digital signing applications.	Managed PKI Service (mPKI)
	End-to-end control for governments and other large enterprises that cannot outsource any aspect of their PKI operation. CLP is a complete on-premises PKI environment that configures and manages digital certificates in a secure and non-reputable manner.	Certificate Lifecycle Platform
	Endpoint, email and file share encryption protects sensitive data, even if it is compromised or accessed by unauthorized persons.	Encryption
DETECT	Detect advanced attacks entering a network through email with unique targeted attack identification and Symantec Cynic sandbox detection.	ATP: Email
	Detect and report on attempts to exfiltrate data, based on policy.	Data Loss Prevention
RESPOND	Synapse correlation technology aggregates any suspicious activity across to quickly identify and prioritize those systems that remain compromised and require immediate remediation. Cynic sandbox detection capabilities to existing installations of Symantec Email Security.	ATP: Email
RECOVER		Other Symantec solutions and services

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec Corporation World Headquarters
350 Ellis Street, Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com
Email: federal_government@symantec.com

SYMC_wp_Government_Insider_Threat_EN_v1a