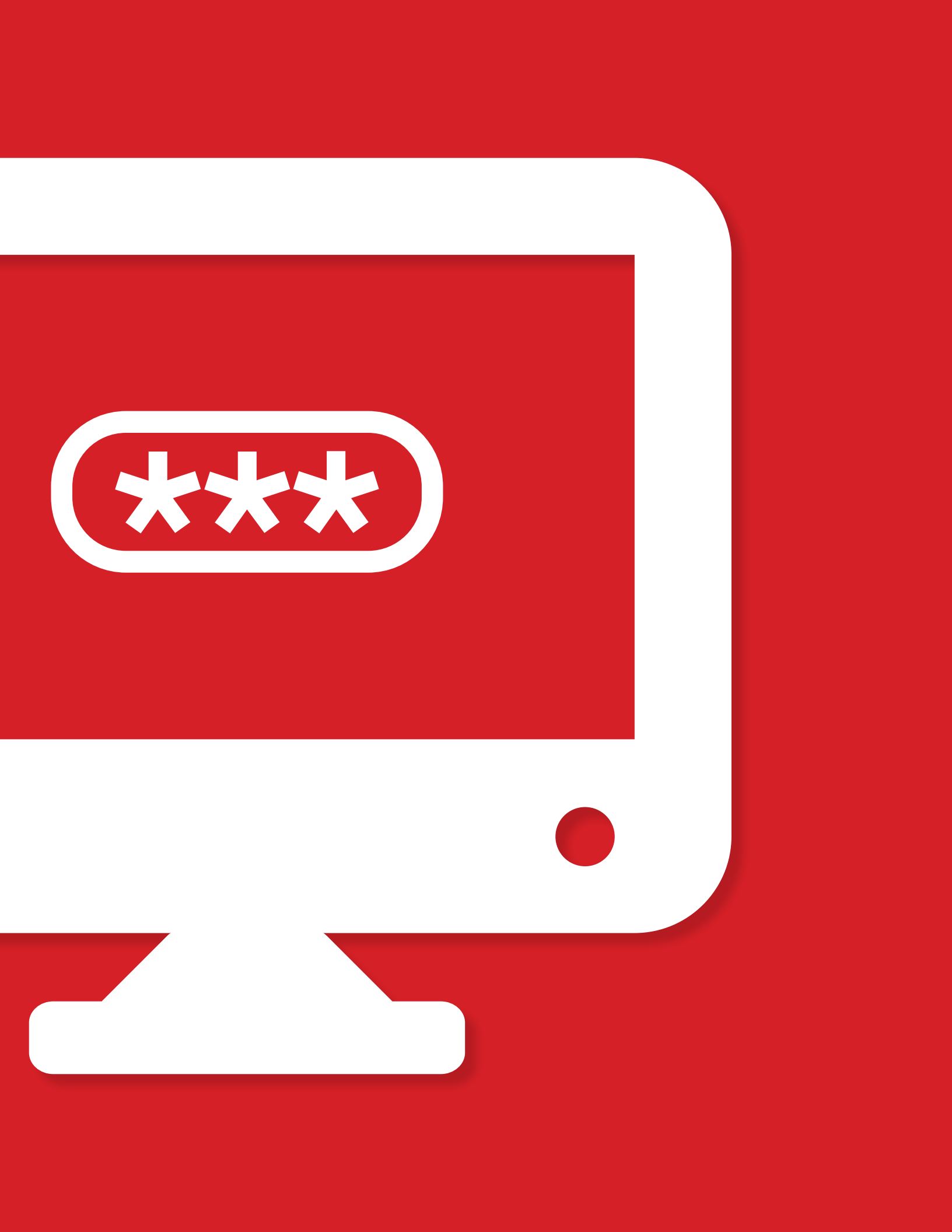
A Better Strategy to Stop Insider Threats

infor

INDUSTRY PERSPECTIVE



"A cyberattack perpetrated by nation-states or violent extremist groups could be as destructive as the terrorist attack of 9/11."

-Leon Panetta, Former U.S. Defense Secretary

The Department of Defense, Internal Revenue Service, Office of Personnel Management, even the White House — what do all of these organizations have in common? Each has suffered a high-profile data breach in the past year. In 2015 so far, the number of people affected by U.S. government cyberattacks has reached an all-time high. From the OPM breach to lesser-known attacks, cybersecurity is rightfully a massive concern for government officials.

Although many cybersecurity conversations have centered on online vulnerabilities, few have adequately addressed the physical threat that individuals with privileged access present. Undoubtedly, the public sector would benefit from greater information technology asset security, but this is only one piece of a much larger security puzzle.

Edward Snowden, Chelsea Manning and other leakers of information before them have proven time and again that it takes only one person to put an entire organization at risk. Identities, intellectual property, classified personnel data, global financial records and even information integral to national security — with all that's at stake, the government cannot afford to overlook the **human element** of information security.

People with access to an organization's most sensitive information who could expose that data are known as **insider threats**. Insider threats now pose perhaps the greatest cybersecurity risk to the government of any information threat.

Who are these people and what can government do to stop them? To understand how to address insider threats, we must first understand where they come from. That's why GovLoop has partnered with Infor, one of the world's leading providers of enterprise applications, to create this industry perspective. In this resource, we focus on the rising challenge of insider threats and how predictive analytics, among other approaches, can help keep government data safe.

Threats Then & Now

Information extracted from security breaches costs the government an estimated $400 billion annually.

Despite making headlines as of late, cyberattacks on the government are nothing new. At the advent of the Internet more than two decades ago, hackers developed the first worms and viruses to infiltrate public-sector organizations. In an interview with GovLoop, Joe Arthur, Infor Public Sector Executive, explained that this first generation of cyberthreats was "more for annoyance than effect."

However, these minor annoyances laid the foundation for a for-profit malware industry targeted at obtaining information for financial gain and IT privileges. Soon, malware progressed to more advanced, persistent threats that hackers could use to pull information over time and then strike where the most damage could be done. These threats, which have allowed criminals to access privileged information in both the private and public sectors, present some of the greatest challenges to the government's information security.

Today, information extracted from government security breaches is expected to result in losses exceeding $400 billion annually. Agencies governmentwide are racing to patch vulnerabilities and mitigate cyberthreats before another attack cripples them. The focus has largely been on bolstering external defense security, but a serious threat to government information remains: insiders.

One-third of all attacks on the public sector are now being attributed to insider threats, Arthur said. Sprawled across the globe with different targets and goals, these highly organized perpetrators are like a mafia. They focus on the weakest links, take advantage of privileged access and use those credentials. This then wreaks havoc on financial markets and national security.

In the past two years, the U.S. Computer Emergency Readiness Team reported that 34 percent of cyber crimes were attributable to insider threats, compared to 31 percent for external threats. The numbers are clear: Insider threats are prevalent across the public sector and the risk they pose to the government's most sensitive information must be mitigated.

But to fully understand how to best defend against and prevent this threat, we must first understand **who insiders are.**

Who is an Insider?

Originally, insider threats were largely constrained to those with privileged access to an organization's sensitive information. However, as information has gone digital and vulnerabilities have evolved alongside technology, the landscape of threats has changed drastically.

Today, an insider could be anyone. It could be employees, a contractor or consultant, a customer, supplier, auditor, or even an actor pretending to be any one of those with hijacked credentials.

Insider threats have exposed the personal data of millions of people in both the private and public sectors. In 2014, for example, eBay was hacked by one employee system logon, which resulted in 233 million eBay usernames, dates of birth, telephone numbers and addresses being made available.

Misusing privileged access to expose sensitive data, using stolen credentials to access a private database or accidentally leaving a USB drive with an organization's sensitive information stored on it at an airport are all examples of an insider threat. Whether the cause is malicious intent or innocent human error, insider threats present a real danger to private- and public-sector organizations.

"What makes these threats so significant is these individuals, depending on their role and privileges, could have access to some pretty significant information that could have a financial impact, an impact for national security…or worse, could jeopardize agents in the field and result in loss of life," Arthur said.

Clearly, insider threats really present a danger that affects everyone. To stop insiders before any more irrevocable damage is done, the government must act to protect its information.

Insiders in the Public Sector Today:

- **Employees**
- **Managers**
- **Federal executives**
- **Contractors**
- **Consultants**
- **Colleges and universities**
- **Foreign allies**
- **Vendors and suppliers**
- **Authorized guests**

Addressing the Insider Threat Problem: What Government Can Do Now

Technology has, of course, been applied to the insider threat problem. However, the government's focus until now has largely centered only on securing data electronically. And although federal agencies would undoubtedly benefit from stronger data encryption and basic antivirus protections, they may not be enough.

To prevent an insider's physical threat to data, the government will have to do more than react to the aftermath.

Because human behavior is so complex, detecting insider threats before they occur can be incredibly difficult. As a result, the government has traditionally been reactive, rather than proactive, when it comes to them. In many cases, by the time officials are aware of a problem, it's already too late.

How can the government respond faster to insider threats? Recently developed network monitoring technology is allowing some network administrators to predict what was previously unpredictable: human behavior. With data science and predictive behavior analytics tools, IT professionals can detect insider threats and even predict likely threats before information is lost, rather than afterward.

Insiders have certain authorization rights and privileges in the organization networks to do their job, which is typically not enough information to derive insiders' intention or psychology in real time. However, over time, you can collect enough of that behavioral information to use for predictive analytics, Arthur explained.

"If you start baselining activities — meaning tracking many different attributes across multiple dimensions — you'll begin to understand normal host behavior, network behavior, user behavior, application behavior, along with other internal behavior like the function of a vulnerability state of the host," Arthur said.

Predicting human behavior seems like a something straight from science fiction, but with proper network monitoring and data analytics, it's not all that difficult. One reason why? In the end, we are all creatures of habit.

The fact is, users are unique individuals and express their different tastes, preferences and work habits in the way they interact with the network. A collection of all those preferences really acts as fingerprints on that network, and each network fingerprint is as unique as the user who generates the traffic."

By collecting and analyzing comprehensive user data, administrators can learn what constitutes "normal" behavior on the network. In fact, when you start looking at data science as a solution to this and you analyze behavioral data, and learn what is "normal," you can build a baseline of activity. Then, once you have a baseline, you'll be able to look for outliers.

"With data science and predictive behavior analytics tools, IT professionals can detect insider threats and even predict likely threats before information is lost, rather than afterward."

Additionally, predictive analytics allow administrators to focus on any anomalies and bizarre behavior, giving them a sense of individual intent and psychology in real time.

Over time, if administrators collect individual user information and get an idea of what typical use looks like for individuals accessing the network, they'll be able to notice when something is amiss. For example, if an individual accesses a database he or she does not normally use and begins uploading sensitive data to a Dropbox account, this would constitute abnormal behavior and a potential insider threat. However, if agencies do not track use on their network, they have no way of knowing what normal use for individuals might be.

A high volume of downloads from internal servers, extensive use of USB sticks, unusual database access, uploads to external drives — all of those are indicators of something that could be used to cast an ongoing attack.

With predictive behavior analytics, government agencies would be able to identify these risky behaviors on their networks and mitigate insider threats before they progress to much larger problems. "We have seen instances where predictive analytics have identified troubled employees and enabled management to step in and help before they took the final irrevocable step," Arthur said.

However, for all its potential benefits, predictive analytics aren't without flaws. For instance, deviations in human behavior do not always indicate malicious intent. Benign changes in behavior such as working longer days to catch up on missed work after a holiday or accessing a different database because of a slight change in occupational role could trigger "false positives" for insider threats.

It is still difficult for computers alone to decipher nonthreatening deviations from the threatening ones. As a result, organizations may have to deal with the fallout from what might be normal network behavior just seeming abnormal out of context. To put those actions in context, agencies will need behavioral science with better data to answer not just what happened, but why.

With thousands of users and millions of data points to collect, government agencies are challenged with allocating enough resources to comb through this overload of information. There is an abundance of tools to address insider threats, but a limited number of resources. As a result, until now most agencies have focused their security efforts on external threats.

Still, by providing administrators a better understanding of what normally happens on their networks, data science and predictive analytics would lend them the ability to spot an insider threat as it happens and stop it in its tracks. As technology advances and new problems emerge, stopping insider threats before information gets out will become increasingly essential for the public sector.

Insiders of Tomorrow: The Next Steps

Proactive Security Strategies:

Manage privileged access

Locate all assets

Use antivirus software

Monitor network activity

Encrypt data

Analyze user behavior

"If you look ahead to the next 10 to 15 years, the advancement of technology makes it impossible to predict that far out. But it is fair to expect that there will be more challenges ahead, borne out of new vulnerabilities that have been evolved," Arthur said. As new technology develops, new vulnerabilities will undoubtedly follow. Threats, both cyber and physical, will be there waiting to exploit those vulnerabilities.

Even in today's cyber landscape, it's clear that the government must pursue strategy to minimize the impact of insider threats and the potential damage. A technology-driven, proactive security approach would help tackle insider threats before their full impact on the government, and ultimately the public, is ever realized.

The resources to stop insider threats are there, agencies just have to use them more effectively. The government must start with basic security practices, including protecting IT assets, encrypting data, evaluating who has privileged access, reinforcing personnel accountability and monitoring network use, Arthur said.

More behavioral science research, tested algorithms and advanced analytical tools would make the government much more effective at getting ahead of the curve. These proactive security approaches would lend government agencies far greater power over their networks and sensitive data than they have today.

To use existing technology to its greatest advantage, Arthur said the government must also refine its policies, procedures and practices to account for changes in overall operations, the international security environment and technological advances.

"If the government can unite, there's enough collective knowledge out there to leverage resources for better information security. The government must just keep in mind that these actions are committed by human beings with certain tendencies and perspectives," Arthur said. Simply monitoring networks to get an idea of these behavioral tendencies would go a long way toward stopping insider threats.

"The expectation, responsibility and authority to practice good security really exist at any level in the government, with every insider and with all government partners," Arthur concluded.

The technology to stop insider threats is there — the public sector just has to use it.

About Infor

Infor is fundamentally changing the way information is published and consumed in the enterprise, helping 70,000 customers in 194 countries improve operations, drive growth, and quickly adapt to changes in business demands. Infor offers deep industry-specific applications and suites, engineered for speed, and with an innovative user experience design that is simple, transparent, and elegant. Infor provides flexible deployment options that give customers a choice to run their businesses in the cloud, on-premises, or both.

http://www.infor.com/industries/publicsector

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 200,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C. with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please email us at:
info@govloop.com

1152 15th St NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com

@GovLoop

1152 15th St NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop