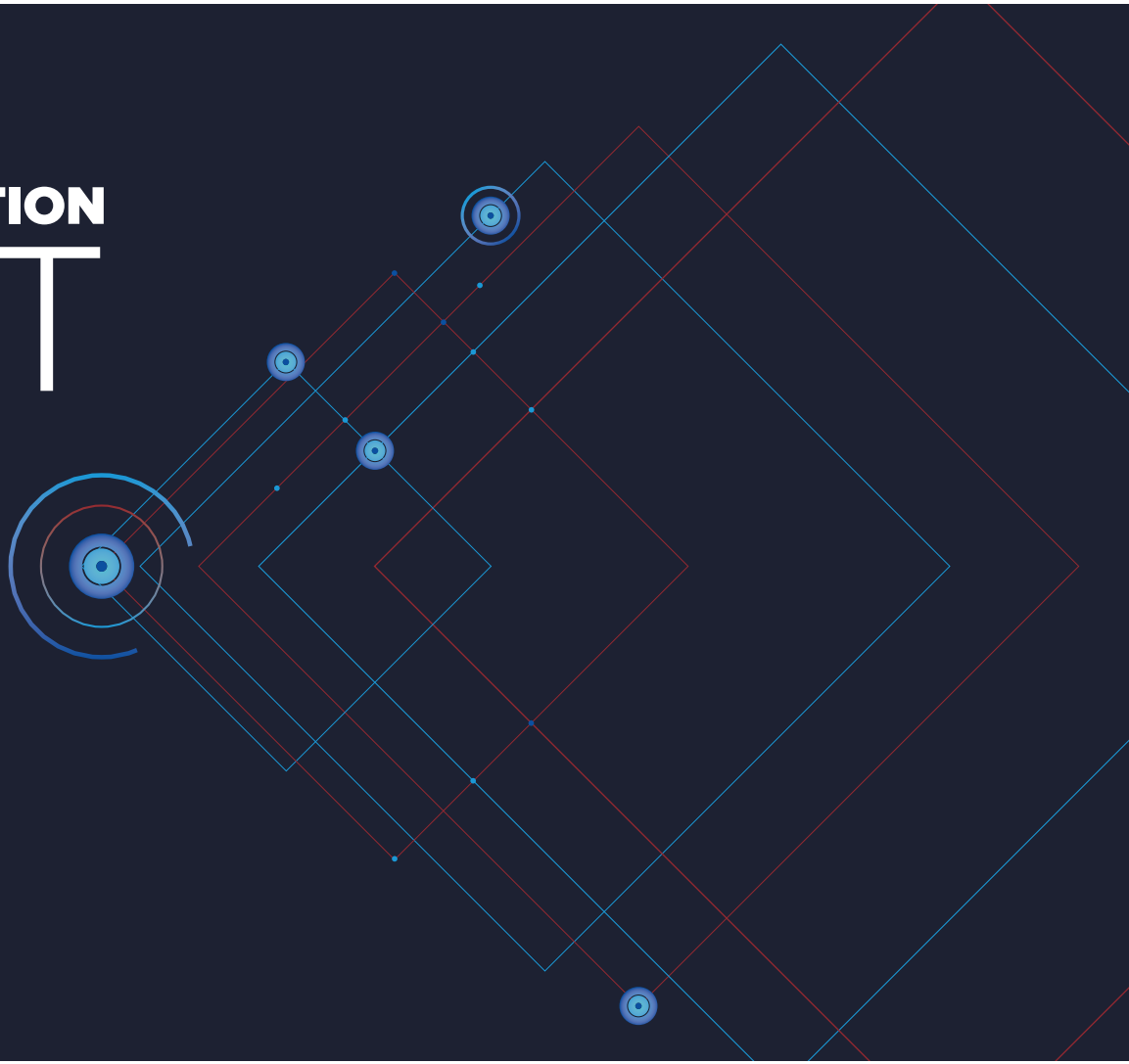
VARONIS

2018

FEDERAL DATA PROTECTION REPORT

Confidence and concern around protecting sensitive data intersect in federal IT and security circles



EXECUTIVE SUMMARY

Federal decision makers are increasingly confident in their agencies' ability to protect data against cyberattacks, thanks to the elevation of data protection as a top strategic priority. This rise in confidence is driven by sharpened awareness and visibility into specific security obstacles and how to best to mitigate them. While agencies have been hit hard by security breaches, a positive learning curve is well underway to better protect sensitive data and systems to ensure success.

To shed light on security challenges within the public sector, Varonis commissioned a survey to explore the perceptions of federal leaders in IT and data security roles. This report reveals growing confidence and prioritization around protecting agency's most critical assets – their data.

Among the Most Notable Findings:

- **Data protection is cited as a top priority by 82%** of federal IT and security professionals
- **More than three quarters** of respondents are confident in their agency's ability to protect against a cyber attack and know who has access to sensitive information
- **43% of federal leaders** indicate they are unaware of any data security incident in their agency over the past 12 months
- Realizing not all threats come from the outside — **nearly half of the IT and security professionals** surveyed have changed security policies and procedures based on insider threats.

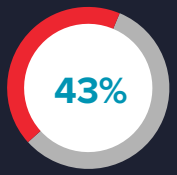
The survey shows agencies increasingly understand the nature of cyber risk in their strategic planning. In ranking their cybersecurity priorities, respondents ranked data protection, cloud security and insider threat detection — at **82%, 55%** and **49%**, respectively — as the top three focus areas in strengthening their systems.

This report positions the survey findings in context of the priorities and obstacles that define the government cybersecurity mission. It also sheds light on pitfalls to avoid and best practices to embrace in shaping an agency's cybersecurity strategy around sensitive data.

Data protection is cited as a top priority by 82% of federal IT and security professionals

MORE THAN THREE QUARTERS

of respondents are confident their agency has the skills, judgment and experience to **protect against a cyber attack (76%) and know who has access to sensitive information (88%)**



of federal leaders indicate they are unaware of any data security incident in their agency over the past 12 months

NEARLY HALF (49%)

of the IT and security professionals surveyed have changed security policies and procedures based on insider threats

THE ENEMY WITHIN

High-profile data breaches are hitting with startling regularity, and many of these incidents involve weak or stolen credentials. In many cases, insider credentials don't need to be stolen — it's the insiders themselves who sometimes turn out to be wearing the black hat, as was the case with Edward Snowden and Reality Winner. Look no further than these two examples and it's clear that the impact of leaked intelligence falling into the wrong hands can be devastating.

Federal IT and security professionals recognize the threat posed by insiders, with **71% indicating** that preventing data access or theft by careless insiders is a significant or moderate challenge to the security of data files and emails in their agency. Of those respondents who had dealt with any security incident, **30% said** that incident involved an insider.

Insiders can do much more damage than an outsider who steals credentials. That's because — along with the access — comes detailed institutional knowledge of an agency's operations that can aid in the theft of intellectual property and other confidential data that can threaten an agency's integrity. This frightening realization underscores the need to safeguard the data within systems not just the increasingly porous perimeters meant to protect the organization from the outside world.

Federal IT and security professionals recognize the threat posed by insiders, with 71% indicating that preventing data access or theft by careless insiders is a significant or moderate challenge to the security of data files and emails in their agency. Of those respondents who had dealt with any security incident, 30% said that incident involved an insider.

THE PROBLEM OF ACCESS

Whether the threat comes from the outside or within, unauthorized access can open troves of data to threat actors. Excessive access to critical assets impacts both the public and private sector.

> *The Varonis 2018 Global Data Risk Report, which examined 6 billion files from a sampling of 130 organizations,* ***found that 58% of companies have more than 100,000 files open to everyone.*** *That figure jumps to 88% among companies that have 1 million folders or more.*

Despite the common experience of dealing with breaches and insider threats, nearly half of respondents said they were very confident their agency knows who has access to sensitive information, while **39% indicated** they were somewhat confident. In fact, **89% of respondents** said they were somewhat or very confident data stored within the agency is secure and protected.

FEDERAL LEADERS TAKE NOTE AND TAKE ACTION

The survey **reveals more than 75%** of federal IT and security professionals are confident that their agency's leadership has the skills, judgment and experience to protect itself from cyber attack, in particular, insider threats.

Further, they have taken concrete measures to improve security:

- **49% indicate** they have changed security policies and procedures as a response to Snowden-style insider threats and;
- **An additional 28% note** they have plans to change that have not yet been implemented.

Amid the flood of digital information within government agencies are vast repositories of sensitive financial data, agency plans, strategic initiatives and confidential employee or citizen records spread across file systems in the cloud and on-premises.

Federal government standards, such as the NIST Cybersecurity Framework, and programs like Continuous Diagnostics and Mitigation (CDM), were designed to help mitigate cybersecurity-related risk to critical infrastructure and the valuable data contained within these systems.

According to the survey, respondents report these initiatives are beneficial and have improved security efforts across agencies:

- **63% of respondents indicate** that federal regulations and compliance requirements have helped their agency improve its user-generated data protection capabilities
- **68% agree** that their agency fully understands the CDM program and NIST Cybersecurity Framework

3 BIG CYBERSECURITY MISTAKES

1. Organizations spend more time and attention protecting networks, systems and supporting infrastructure than they spend on protecting the data their infrastructure was created for. That's like protecting the refinery but forgetting the oil.

2. Too much focus on preventive technologies, such as antivirus and firewalls, leaves organizations vulnerable to evolving threats. Agencies must be in the position to detect when an insider is compromised and respond quickly.

3. The approach to data security has been fragmented and reactive instead of strategic. In a recent study, Forrester calls this "expense in depth," causing 90% of data security professionals to experience persistent technical challenges, including keeping up with evolving cyber threats and dealing with disparate systems that don't communicate. The result is a failure to reduce meaningful risk.

DATA SECURITY BEST PRACTICES UNDER THE NIST FRAMEWORK

The NIST Cybersecurity Framework has been widely adopted to help secure critical infrastructure and government networks, but NIST is also an excellent foundation for building a robust data protection strategy. Adopting NIST will help you comply with data protection regulations, ensure your sensitive data is not overexposed, and that your overall data security risk is minimized.

Would your organization's data security approach stand up to the NIST framework?
Here are some best practices for each of the five core functions.

IDENTIFY

With large volumes of data spread across disparate data stores, most organizations aren't able to spot misconfigurations, where their data is exposed, and what data is sensitive. The Identify function is all about "turning on the lights" in the environment.

Classify sensitive data, pinpoint and monitor privileged accounts, and map directory services (like Active Directory) and file systems to get context about users and their roles, what data they can access, how they get access, and where they have access across a multitude of servers or disparate platforms.

PROTECT

A primary of the Protect function is to prevent and limit the potential damage of future breaches by locking down sensitive and stale data, reducing broad and global access, and simplifying permissions. Start by remediating your biggest risks first—such as sensitive information exposed to global access groups and removing users from privileged security groups they don't need to belong to in order to do their jobs.

DETECT

Enable activity auditing on supported platforms to collect all file and email access events as well as Active Directory changes. Establish a baseline of each user's activity on file systems, email, active directory and other systems to identify deviations that indicate unusual, unwanted or malicious activity.

Insider threats and attackers that circumvent perimeter controls are difficult to detect with telemetry from perimeter devices and signature-based security systems by themselves. Files and email are targets in most attacks, and are easier to detect by observing and analyzing behavior patterns on the file and email systems themselves.

DATA SECURITY BEST PRACTICES UNDER THE NIST FRAMEWORK CONT.

RESPOND

Once a system is in place to alert on suspicious data access, it becomes critical for IT and security staff to have plans in place for investigation and response. Providing a playbook allows staff to follow a consistent, repeatable, process to determine if alerts constitute a breach, and how to react if a breach is discovered – both to recover from an incident, and how to notify the proper individuals in the company for regulatory compliance.

RECOVER

Just as NIST is ever-evolving, so must your security policies and technology. It's vital to put systems in place to ensure that detective and preventive controls are maintained, that newly stale data is retained or disposed of automatically, that sensitive data is automatically quarantined if necessary, and that behavior continues to be monitored for new threats. What's more, access should be reviewed and recertified on a regular. Gone are the days of getting an authorization and not revoking access long after the need expires.

Compliance with NIST is a perfect starting point for any data security strategy. The new GDPR regulations shine a spotlight on data security compliance guidelines in Europe, and changes are already coming to state legislation in the U.S. that will implement *additional* requirements. As new legislation rolls out, achieving and maintaining compliance with the current baseline will make much easier to meet updated requirements.

CONCLUSION

Federal IT and security professionals face a daily struggle to prioritize multiple initiatives to ensure success. Competing organizational priorities were cited as the number-one factor complicating agency efforts to manage, secure and protect data.

Safeguarding data is the foundation of effective cybersecurity. A sound data strategy can increase efficiency and protect agency assets as the federal government works to serve citizens in a world of growing threats and shrinking resources.

About the Report

The 2018 Federal Data Protection Report captures responses from 150 federal government decision makers (75 from civilian agencies and 75 from defense) in an online survey conducted by Market Connections and designed to explore federal government decision makers' and influencers' attitudes and awareness surrounding sensitive data.

The blind online survey was administered over a ten-day period in March 2018. All 150 respondents are involved in their organization's decisions or recommendations regarding IT data security and/or enterprise data solutions. Statistical analyses were conducted for agency type (civilian vs. defense); however, there were no notable significant differences to report between these two agency types.

About Varonis

Varonis is a pioneer in data security and analytics, specializing in software for data security, governance, compliance, classification, and analytics. Varonis detects insider threats and cyber attacks by analyzing file activity and user behavior; prevents disaster by locking down sensitive data; and efficiently sustains a secure state with automation.