SecureWatch for Government

RiskWatch

Government Risk Management

Government departments are assessing risks today, but often at minimal efficiency due to industry restraints. We regularly see a dated and manual process of using excel sheets, written reports, and file shares to manage risk and compliance. However, despite the complexity of the risk management required, many must struggle to mitigate risk at a price their employers are willing to pay. This typically results in incomplete or rushed assessments that leave government departments vulnerable to threats.

What's more, government departments and agencies face an ever-increasing amount of pressure to improve transparency in their processes. As part of this, risk management becomes a key point of focus in the public eye. In the face of an emerging threat or crisis, the public will seek verification that government departments took the necessary steps to reduce risk and promote business continuity.

With privacy and security at the forefront of government challenges, what steps are being taken to mitigate risks? Unfortunately, it would seem that whatever those steps may be, are often not enough. A report by Thomson Reuters shows that nearly a quarter (24%) of departments are outsourcing all or part of their compliance and risk assessment functionality. This increases costs without training existing staff on proper procedure.

Lets look at some of the biggest risks in government today and highlight the importance of communicating risk appetite and tolerance across an organization. In addition, we will explain how the SecureWatch platform can assist in addressing these pain points.

Top Government Risks

The following are four of the biggest risks facing government today. As with any industry, risks may reduce with proper attention to data collection, analysis, and creating action plans. Over time, you will begin to notice how risk is reducing and compliance is improving, as well as the benefits these bring to the work place.

Outdated Technology

First, aging IT systems are a major security risk that plagues the federal government. It's simple understanding that old systems don't have the capabilities to protect against threats that weren't around when they were created. Technology is constantly advancing, and yet government technology is at a crawl, requiring a lot of resources to keep systems running. A 2016 report from the Government Accountability Officeshows that 75% of the total IT budget was spent on operations and maintenance.

Not only is government use of outdated technology using up the majority of their resources, it is leaving them vulnerable to modern threats and attacks. Several servers used at homeland security, for example, reportedly used Windows Server 2003 for nearly 3 years after it was no longer supported.

In 2018, Hawaii residents received a false missile alert that gained a lot of media attention. While the missile crisis sparked some debate on whether it was truly an accident or not, the incident offered insight to the software. Initial reports claim the alert was sent on accident due to the aging technology not making a clear distinction between the real and practice alert. Reports also say the command's operations center didn't have access to the alert system during the event, resulting in a 38-minute period before another alert was released.

Cyber Security

Cyber security deserves its own category in every industry. When discussing government cyber security though, we have well warranted cause of concern. Government agencies store a lot of valuable data, and a lot of it is about the public: driver's license information, social security numbers, health care information, financial data, etc. It makes sense they would be a large target for today's more sophisticated cyber attacks. Is the government prepared though?

In 2015, the Office of Personal Management announced two separate cybersecurity incidents, resulting in the loss of over 25 million individuals' information such as social security numbers. In 2016, hackers breached a data retrieval tool at the IRS, allowing them to steal 30 million dollars and access the personal information of 100,000 students. In 2018, the Chinese government hacked Navy computers, stealing 614 gigabytes of sensitive information related to undersea warfare. These incidents are largely worrying, and a report by Netwrix shows that only 14% of government organizations consider themselves properly protected against cyber attacks.

Employees

Government employees present a large risk to security that is often overlooked. Processes that leave room for human error are numerous in any organization, often due to issues in training and poor work habits. This is often a result of poor work culture. We find too often that risk management and compliance is simply a task to check off and not an ongoing dialogue of ensuring proper education.

A 2014 report states that only 27% of U.S. federal government workers are engaged in their jobs. In addition to costing an estimated $18 billion a year in productivity, this raises red flags for risk. Employees who are not engaged in their work or put effort towards following work policies are likely to cause issues with compliance and result in work disruptions, legal fees, and workers comp claims. In 2016, government entities reported that human error was the cause of 57% of security incidents and 14% of system downtime.

Infrastructure

Infrastructure risk is the potential failure of organizational structures and facilities, and loss of their services. As the Department of Homeland Security says, “The nation’s critical infrastructure provides the essential services that underpin American Society.” These assets are necessary for both physical and economic security, as well as public safety. In 2018 President Trump signed the Cybersecurity and Infrastructure Security Agency Act of 2018, which established the Cybersecurity and Infrastructure Security Agency (CISA). Field assessments are performed by CISA to identify vulnerabilities within the nation’s critical infrastructure.

CISA reportedly works to identify the most critical risks to U.S. infrastructure across 16 sectors, utilizing resources and collaboration from the National Risk Management Center (NRMC), which is housed within the organization. We put our faith in departments such as these, who protect against the unimaginable. Whether physical or cyber in nature, an attack on the U.S. power grid or industrial control systems is a threat that could cause potentially catastrophic results. How quickly could we rebound from the loss of power?

Risk Callout

75%

75% of Government IT budget is spent on operations and maintenance, instead of implementing newer and safer technology.

14%

Only 14% of government organizations consider themselves properly protected against cyber attacks.

73%

73% of government employees report that they are not actively engaged with their jobs.

57%

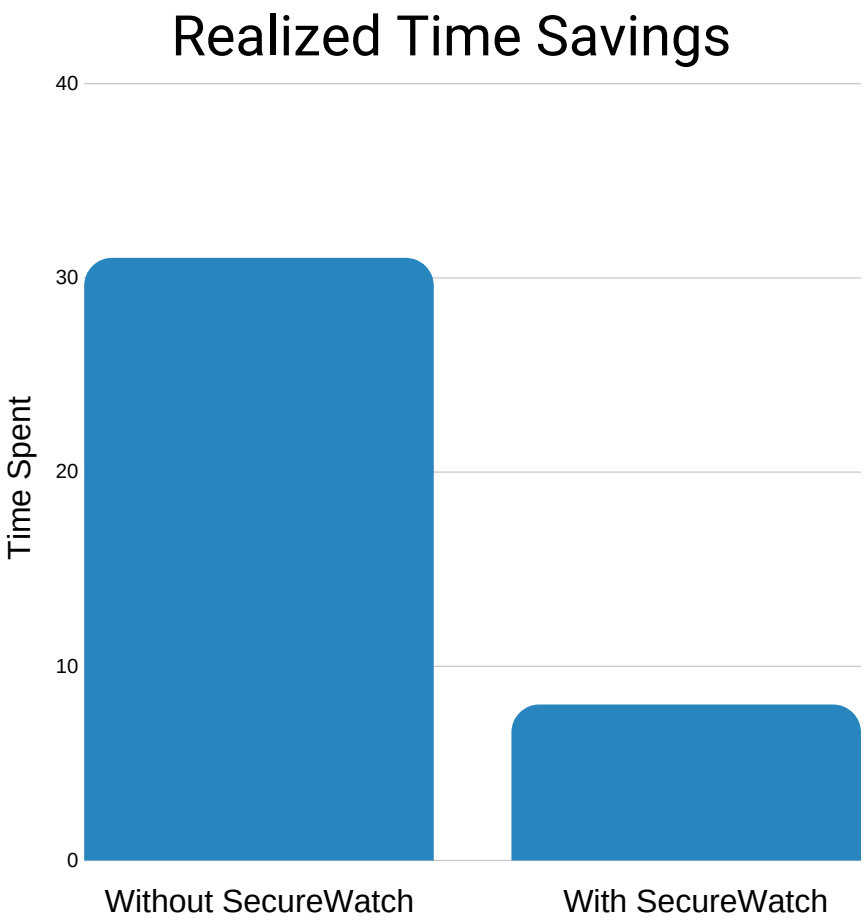
57% of government security incidents were reportedly caused by human error.

SecureWatch increases your organization's ability to detect, predict, and appropriately respond to any signs of potential risk.

RiskWatch for Compliance and Risk Management

Our tool SecureWatch provides an affordable and effective method to managing your risk and compliance. SecureWatch is a cloud-based solution for conducting inspections, audits, and risk assessments. Measurable data allows you to measure compliance and create a business case for investments to protect your assets and image.

We realize the specific needs of government employees, so we've designed key features of our platform to make your job easier. SecureWatch excels by helping you complete your assessments an average of 74% less time than a manual system, allowing you to cut costs in your assessment process without sacrificing precision. Your extra time allows you to complete more assessments or other activities. Below, you'll see a simple time savings chart showing the contrast.



Key Features

Customized Assessments and Reports

Simply select which regulations and standards you want to measure compliance with and the questions will be added to your survey. You can edit the questions and how they are answered to better fit your needs. Reports can be customized to mimic your current report layout and with white labeling.

Compliance Reporting

With the click of a button, create an auto-generated report showing the status of any assessments you've completed. Utilize this to track policies/documents and easily gain insight into problem areas with suggested remediation and any supplemental photos.

Assessment Ease of Use

The software sends introductory emails to anyone that will be completing an assessment and explains how to complete their task. Assessment management is automated with reminder emails that are sent to users that have not completed their assignments and the software will email an admin if there is continued lack of progress.

Dashboard Overview

Quickly look at your dashboard to see an overview of your risk scores across all locations, letting you know where to focus your attention and resources.

A key benefit of our solution is that outsourcing is no longer needed to complete assessments. We offer over 35 content libraries that our content specialists have converted to an easy-to-answer survey format. This allows any staff member to complete assessments, and even helps them become more familiar with the regulations or standards they are assessing against.

Even tracking results and planning your next steps is simplified. SecureWatch allows you to replace subjective analysis with objective criteria in a defined and structured process that promotes tracking improvement over time. The guess work in evaluations is removed and you can see exactly what areas you need to improve, providing the transparency that is so valuable in government. Release auto generated reports showing your compliance and level of risk, per the results of your assessments.

RiskWatch offers free trials and a consulting service to assist in performing a proof of concept using any of its assessment platforms. Manage all types of risk from across your business through a single, securely accessed, web-based tool that reduces risk and improves operational effectiveness and efficiency.

Try it Now

RiskWatch
Global Leader in Risk Assessment Solutions