AKIMA

WHITEPAPER

New Cyber Realities Require a New Approach

To stay a step ahead of adversaries, savvy IT security professionals vigilantly monitor and analyze the cyber landscape, mitigating known hazards and nimbly shifting tactics to neutralize threats that mutate with the adroitness of drug-resistant viruses.

If it's been a while since your agency underwent a cybersecurity checkup, chances are that you're overdue for either a system-wide security assessment or some really bad news. Compared to a few years ago, government agencies are experiencing more ransomware and business email attacks, more man-in-the-middle attacks, more cross-site scripting, and more zero-day exploits. In the unpredictable world of cybersecurity, the status quo just doesn't cut it.

The type and volume of threats have changed, and agencies' attack surfaces have expanded. As with civilian organizations, federal and military agencies continue to deploy more internet-enabled devices that can be vulnerable to distributed denial-of-service (DDoS) attacks. At the urging of the administration and government leaders, agencies are moving aggressively to the cloud – and drastically changing requirements for data encryption and application security as a result.

Consequently, traditional defense in depth strategies that protected agencies' networks for many years are, in many cases, no longer the best approach.

"A defense in depth cybersecurity strategy typically assumes that there is one point of entry or exit in a network," explains Carrie McLeish, senior IT solutions architect at Akima, a federal contractor with extensive cybersecurity expertise. "That doesn't work well anymore. Even if you build a great fence around your network, hackers can find five ways around it – through an IoT device, a cloud-based application, a weak password or any number of other ways."

> As the sophistication of technology and hackers advance, agencies must become nimbler, more assertive.

Federal oversight groups concur. A report issued in late 2018 by the General Accountability Office (GAO) found that in 2017, the most recent year for which figures are available, federal agencies reported[1] more than 35,000 information security incidents, an increase of about 14 percent from the previous year. These incidents resulted from improper usage, loss or theft of equipment, email/phishing, and other methods used to attack networks.

A report[2] from the Office of Management and Budget (OMB), also released in 2018, found that most agencies were at risk or high risk of cybersecurity breaches. Reasons cited in the report include insufficient capability to detect and investigate attempts to access large volumes of data, sparse threat information, and gaps in network visibility.

[1] *gao.gov/assets/700/696105.pdf*

[2] *whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf*

The New Cyber Reality

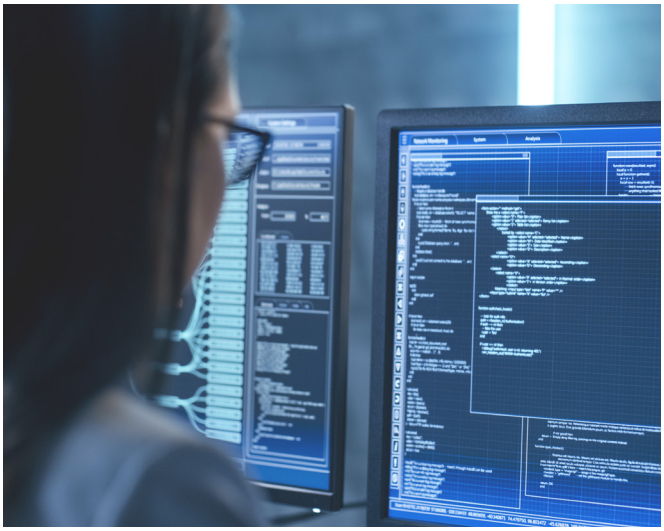
Clearly, the old ways of keeping federal networks and data secure are no longer adequate. It used to be standard practice to buy and install cyber protection technology based on the static state of infrastructure, requirements and data, a strategy that provides protection only until something changes.

"You have to know so much to stay secure today," McLeish says. "You have to know where the network boundaries are, what part of the network agencies own and operate themselves and what part is outsourced, how agencies get their services, how they access data, where they store data, and how that data is protected. You also need to know which data is high-value and sensitive."

Conducting a forensic analysis of assets is just the beginning. With a current understanding of the environment, cybersecurity experts can calibrate the tools agencies use to protect data, applications and people, integrating additional tools as needed. Staying ahead of shifting threats calls for a combination of artificial intelligence and analytics.

"One of the best ways to understand anomalies in your environment is by analyzing the logs of your application and tools, but it's a never-ending job, and there is such a huge volume of data that it's difficult to figure out how to correlate it all," McLeish explains.

The scope of the challenge has made artificial intelligence and analytics increasingly important. These technologies quickly analyze huge volumes of data, comparing multiple logs to provide insights not readily available to un-aided human analysis. Humans are well-equipped, however, to act on concerns identified by computer-assisted analysis, changing policies or mitigation strategies to address identified issues.



> *"Every environment and every tool requires continuous assessment and updating.*
>
> – Carrie McLeish, Senior IT Solutions Architect, Akima

Configuration and Change Management

In addition to continuous systems analysis, an effective cybersecurity strategy includes ongoing configuration and change management.

Threat mitigation strategies must be ongoing because the cyber environment threats change constantly. In a typical month, one arm of a government agency might add a paycheck monitoring tool, while another adds a tool to manage constituent records. A third department might add dozens of internet-enabled devices to the network. By the end of the month, the agency might have added quite a few new tools, each with specific vulnerabilities and with logs that must be correlated and analyzed. Ensuring that these new tools don't pose security problems requires proper configuration and management. Over time, adding new tools to the network could require changing the configuration and management of existing tools.

To keep up, cybersecurity professionals must always know what's on the network and how it is changing. Automated tools and monitoring by third-party service providers are potential options depending on mission requirements, budget, and data sensitivity.

Additionally, adopting a standard cyber security framework, such as NIST's Risk Management Framework[3] helps agencies to manage cybersecurity risks using accepted best practices and processes. Akima is currently using RMF to ensure that DoD medical devices at the Office of Surgeon General for the U.S. Army and U.S. Army Medical Command can connect to their network without creating unnecessary cyber security risks.

> **In cybersecurity, there is but one constant: threats, technologies, and priorities always change.**

"There is no more 'set it and forget it,'" McLeish says. "Every environment and every tool requires continuous assessment and updating. Intelligent, ongoing analysis is the best way to achieve that. It's the only way to be informed about protection of your and mitigate risks of data manipulation as they occur."

[3] *csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview*

Bolstering Cyber Defenses

Akima delivers end-to-end cybersecurity services that help agencies detect, analyze, relate, mitigate, and remediate cybersecurity threats while fully leveraging their existing security investments. Our experts work across multiple platforms and technologies and offer an integrated approach to:

- Insider Threat
- Cloud Security
- BYOD
- Big Data Security
- Intrusion Detection/Prevention
- Incident Response
- Information Assurance
- Auditing
- And more

Its cyber *simplified.* To learn more, visit akima.com.