Addressing Resource Limitations with Automation

Highlights from the "Cyber Compliance Boosted by Automation" Webinar

On March 9, 2021 The Advanced Technology Academic Research Center (ATARC) and Red Hat held a joint webinar on the topic of "Cyber Compliance Boosted by Automation" featuring a panel of eminent participants: Ted Okada, Chief Technology Officer (CTO) of the Federal Emergency Management Agency (FEMA), Dr. Kathleen Kaplan, Chief Data Officer (CDO) of FEMA, Kenneth Clark, CDO and Assistant Director of U.S. Immigration and Customs Enforcement (ICE), and Sebastian Dunne, Principal Solution Architect at Red Hat. While the conversation covered a variety of topics, three of the most prominent were:

- the imperative to protect sensitive information,
- the staffing limitations faced by organizations in the public sector, and
- the advantages of automation for security and compliance.

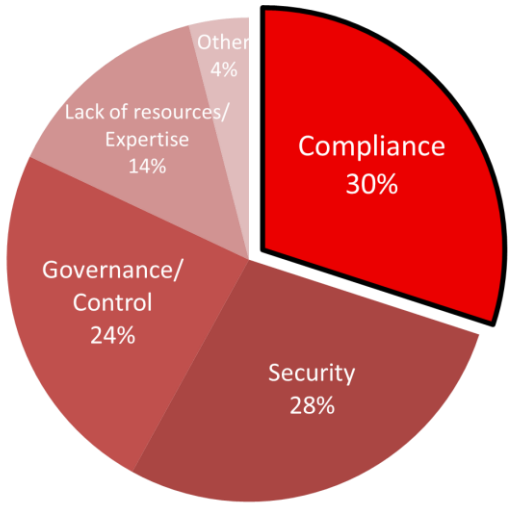
Understanding the Scope of the Challenge

With the continued challenge of responding to the coronavirus pandemic top of mind, Kaplan noted that many of FEMA's 300,000 employees work in the field, directly helping American families respond to not just the pandemic but also to natural disasters such as hurricanes, tornadoes, and earthquakes. As such, the hundreds of thousands of men and women who work at FEMA need to be vaccinated in order to protect both themselves and the everyday Americans with whom they work. The agency has set an ambitious internal goal of an 80% vaccination rate among its staff, requiring an enormous effort both internally and in conjunction with vaccination partners. Okada added that this was not something uncommon for FEMA: much of the agency's work entails close cooperation with other agencies and organizations.

> *A lot of the work we do at FEMA is actually inter-agency. We partner with states, cities, tribal territories, and even nonprofits like the Red Cross to accomplish our mission. That requires sharing data but we need to ensure that we do so in a responsible fashion.*
>
> Ted Okada
> CTO of FEMA

Such cooperation may require the sharing of personal identifiable information (PII), so FEMA has to take great pains to ensure that information is only transferred in compliance with the organization's strict security guidelines. Kaplan pointed to FEMA's strong internal data governance council as being critical to this effort. Clark noted that similar challenges exist at ICE. Given the sensitive nature of the data the agency has access to, such as healthcare records, there is a need to understand exactly who accessed what data and whether they did so for a legitimate purpose. Audience participants shared many of these concerns, with participants pointing first to "compliance" (30%), followed by "security" (28%) and "governance/control" (24%) as being the biggest challenge of managing machine identities across hybrid cloud environments within their agencies.

Webinar Audience Poll: What is the biggest challenge of managing machine identities across hybrid cloud environments in your agency?

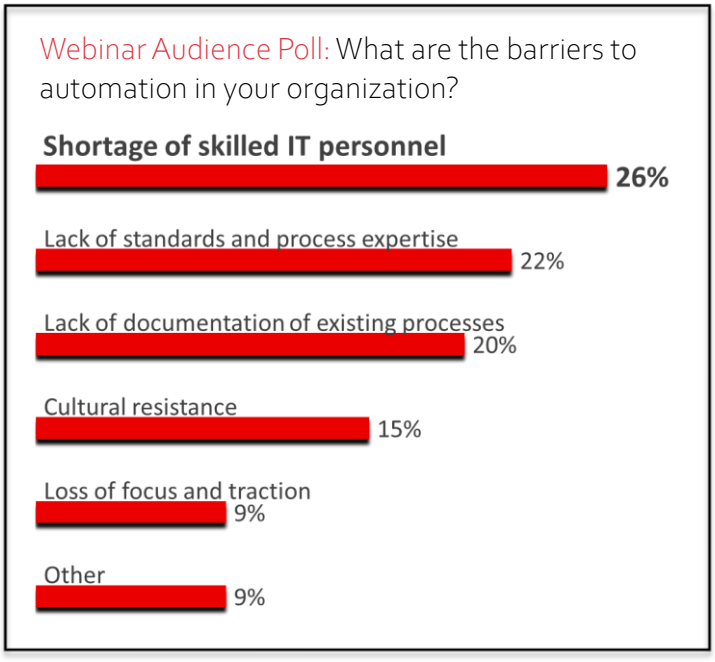


Overcoming Resource Limitations & Leveraging Automation

Another important barrier cited by participants was a "lack of resources/expertise," a common problem in the public sector. Kaplan spoke at length about the challenge of finding qualified staff willing to go through the lengthy hiring and screening process required to gain employment at a federal agency. To make matters worse, federal hiring schedules are often unable to respond as quickly as needed to changes in the technology landscape and mission objectives.

> *Government hiring does not change as quickly as changing requirements. It can be a challenge to find qualified candidates who are willing to wait the process out. We have to get creative in hiring people into positions that don't formally exist, even if they really should.*
>
> Kathleen Kaplan
> CDO of FEMA

The end result is that Kaplan and agency leaders like her are forced to "beg, borrow, and steal" the resources they need and find ways to hire personnel with relevant skills within existing schedules, even if these are outdated. Audience participants clearly saw the same problem, with a "shortage of skilled IT personnel" being the leading factor cited as inhibiting the adoption of automation technology.



However, Dunne pointed out that automation doesn't need to be particularly advanced or resource-intensive in order to be effective. In fact, automation can often free up personnel for more critical tasks. By way of example, Dunne pointed to his experience leading a team of network engineers at an education nonprofit. Dunne noted that in his time there, malicious probes on the nonprofit's firewalls were a common occurrence at all hours. Yet even an attack that was relatively routine and easy to detect would require manual intervention from an administrator.

Another pain point was the need to manually implement security baselines, a process that was not only incredibly time-consuming but also error prone; even the most skilled engineer or administrator could eventually make a mistake. Even once the baselines were implemented systems could still drift out of compliance. Today this challenge is addressed by leveraging the community-developed Security Content Automation Protocol (SCAP), which converts security baselines into machine-readable text that can be deployed in an automated fashion.

Charting a Path Forward

As a Red Hat customer, the Department of Homeland Security, the parent department of both FEMA and ICE, is able to get the benefits of automation without a large investment in staffing. This is because the Red Hat Ansible Automation Platform automatically invokes the agency's action when a threat is detected. Developers and business users are given access to the automation governance they need in order to meet compliance requirements. Ansible customers also gain access to Automation Analytics, a SaaS-based solution enabling operations team members to analyze and aggregate data and generate reports on the status of automation deployments.

To learn more about Red Hat Ansible Automation Platform, please visit: https://www.redhat.com/en/technologies/management/ansible.