5 Ways the Cyber EO Will Change How Govies Work

The Biden administration's Executive Order on Improving the Nation's Cybersecurity made headlines in spring 2021 with its commitment to zero trust security, multi-factor authentication, information sharing and other key cyber policies. The ramifications of the EO go beyond agency policymakers – and in some cases extend to state and local agencies well.

This resource, developed in conjunction with Alcatel-Lucent Enterprise, explores five areas in which the Cyber EO will influence how govies work and how their agencies think about cybersecurity.

govloop

Alcatel·Lucent Enterprise

1 How agencies respond to cyberattacks

Cybersecurity is all about failing forward. Whenever an incident happens, the goal is to learn from what went wrong. But we can learn from other people's mistakes as well.

This approach has helped improve safety in the transportation industry. The National Transportation Safety Board was created to investigate accidents in aviation and surface transportation and provide safety recommendations that can prevent future accidents.

The Cyber Safety Review Board, instituted by the EO, will play a similar role in cybersecurity, investigating significant cyber incidents and recommending actions for improving cybersecurity and incident response practices and policy.

Federal and private-sector co-chairs will run the board. Other representatives will come from civilian, military and intelligence agencies. The secretary will also select representatives from private-sector cybersecurity and software suppliers. This diversity ensures the board's suggestions accurately reflect the national identity.

2 How agencies track cybersecurity events

Network and system logs might sound far removed from the concerns of most employees. But those logs can provide essential insights into what's happening on a network.

Various network and system software and hardware automatically generate voluminous logs about network activity. The right analytic tools, increasingly aided by artificial intelligence and machine learning, can sift through all that information and identify key anomalies or patterns that might indicate a threat.

It's like having an air traffic control radar but for cyberthreats. The problem is that a lot of agencies are not disciplined in how they capture, store and use that data. Instead, they are flying blind. The EO seeks to change that.

As part of the EO, the Homeland Security Department (DHS) is leading an effort to define requirements for maintaining logs and other relevant data. That includes:

- **The types of logs to be maintained**
- **The time periods to retain the logs and other relevant data**
- **The time periods for agencies to enable recommended logging and security requirements**
- **How to protect logs**

All this activity is happening behind the scenes, so most employees will not be aware of it. But such capabilities can reduce the damage and disruption that we all experience from cyber incidents.

3 How agencies buy software

In recent months, everyone has gotten an education in the vulnerability of the global supply chain that ensures the delivery of goods to our nation's economy. The result? Empty shelves, slow deliveries and rising prices.

The software that agencies buy has its own supply chain, with its own vulnerabilities that can pose serious risks to critical systems and data.

The problem is that when an agency buys software, they often don't have visibility into the source of all that code and the tools and processes used to develop it. They can't be sure that the software does not include hidden gaps (intentional or not) that malicious exploit.

Among other actions, the EO calls for:

- **The National Institute of Standards and Technology (NIST) to publish guidance outlining security measures for critical software to be used with future software buys**
- **NIST to identify secure software development practices or criteria for a consumer software labeling program, in line with the widely used Energy Star program**
- **Vendors to provide customers software bills of material that provide details on the various components used to build their software**

4 How agencies think about their data practices

When it comes to data security, it's easy to fall into the trap of thinking in terms of two big buckets: classified and unclassified data. But it's not that simple.

Some datasets, while not classified, are more sensitive than others and at higher risk of attack. For example, while the theft or exposure of administrative data would create a lot of headaches, more damage would be done by the breach of operational data or personally identifiable information or protected health information. Malicious actors understand the difference, and they act accordingly.

Agencies need to think like cyber criminals. Rather than treating all unclassified data as the same, the EO directs agencies to identify their highest risk data sets and to identify data processing and storage solutions that address that risk.

It's worth noting that the EO also raises the baseline for data security. At present, some organizations protect their most sensitive data by encrypting it both in storage and in transit. They also might deploy multi-factor authentication (MFA), requiring users to verify their identities in several ways, such as a combination of password and token (e.g., a common access card).

5 How employees access network resources

The concept of zero trust security often seems remote from the daily work routine of agency employees. But as agencies roll out zero trust, employees will notice.

The guiding principle of zero trust security is "never trust, always verify." In traditional networks, users whose identities have been authenticated at the network perimeter are assumed to be trustworthy and given a wide range of resources on the network.

In zero trust, every user and device on the network is seen as a potential threat, so their access to resources is limited and their identity, permission levels and security status are continually verified. Further, a network can be divided into micro-segments that limit the ability of a user or device to move from one part of the network to another.

One of the most important aspects of zero trust security, from an employee's perspective, is the concept of least privilege. Least-privilege access means that employees (and their devices) should be given access only to those resources that they need to do their jobs.

How to Prepare for the Worst

The EO developed two Cybersecurity Incident and Vulnerability Response playbooks, courtesy of DHS's Cybersecurity and Infrastructure Security Agency (CISA) – one for incident response and one for vulnerability response.

CISA's objective was to provide agencies with a standard set of operational procedures to be used in planning and conducting cybersecurity vulnerability and incident response activity, so that other agencies don't have to figure it out for themselves.

Here are some of the steps that agencies should take to prepare for major incidents before they occur:

- **Documenting and understanding policies and procedures for incident response**
- **Instrumenting the environment to detect suspicious and malicious activity**
- **Establishing staffing plans**
- **Educating users on cyber threats and notification procedures**
- **Leveraging cyber threat intelligence (CTI) to proactively identify potential malicious activity**
- **Define baseline systems and networks before an incident occurs to understand the basics of "normal" activity (making it easier to identify deviations)**
- **Having infrastructure in place to handle complex incidents, including classified and out-of-band communications**
- **Developing and testing courses of action (COAs) for containment and eradication**
- **Establishing means for collecting digital forensics and other data or evidence**

Conclusion

The Cyber EO is not about quick fixes; it's about institutionalizing technologies, processes and policies that can improve cybersecurity over the long run. That said, don't be surprised in the coming months as your agency begins implementing some of the tactics and strategies mandated by the order. **Just remember: Better security is in everyone's best interest.**

Agencies don't have to tackle cyber alone. Alcatel-Lucent Enterprise (ALE) provides industry-certified network solutions serving civilian and defense agencies. ALE is prepared to help agencies meet the mandates of the EO, including the implementation of zero trust macro and micro network segmentation. To learn more, visit: https://www.al-enterprise.com/en/industries/government/usa-federal.

LEARN MORE

govloop

Alcatel·Lucent Enterprise