arcserve®

Data Resilience, Cybersecurity, and Compliance in the Age of AI

Table of Contents

White House Announces National Cybersecurity Strategy: What It Means for Your Business

Ransomware and cyberattacks are making headlines daily. And with the U.S. and the rest of the world now dependent on data to keep things running, cybersecurity and data resiliency are more critical than ever. As a result, the Biden-Harris administration has announced a National Cybersecurity Strategy that intends to "secure the full benefits of a safe and secure digital ecosystem for all Americans."

Rebalance and Realign Cyberspace Defenses and Incentives

The strategy calls for a fundamental shift in how the U.S. allocates cyberspace roles, responsibilities, and resources. It includes efforts to "rebalance the responsibility to defend cyberspace away from individuals, small businesses, and local governments and onto the organizations that are most capable and best-positioned to reduce risks for all of us."

At the same time, the strategy states that the country "must realign incentives to favor long-term investments by striking a careful balance between defending ourselves against urgent threats today and simultaneously strategically planning for and investing in a resilient future." The announcement goes on to say that "the strategy recognizes that government must use all tools of national power in a coordinated manner to protect our national security, public safety, and economic prosperity."

Intentional, Coordinated, and Well-Resourced Approach to Cyber Defense

The announcement provides an overarching vision that addresses the complex threat environment in which we live and how we secure the promise of our digital future. The statement goes on to say that this vision will be realized as the U.S. and its allies and partners make our digital ecosystem:

- *Defensible, where cyber defense is overwhelmingly easier, cheaper, and more effective*
- *Resilient, where cyber incidents and errors have little widespread or lasting impact*
- *Values-aligned, where our values shape and are reinforced by our digital world*
- *Cybersecurity Strategy Built on Five Pillars*

The Biden Administration's approach to fulfilling this strategy is built on five pillars:

1. Defend Critical Infrastructure

This pillar is intended to give Americans confidence in the availability and resilience of our critical infrastructure. Its focus is expanding minimum cybersecurity requirements in critical sectors, enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services, and protecting and modernizing federal networks and incidence response policies.

2. Disrupt and Dismantle Threat Actors

The administration will use "all instruments of national power" to prevent malicious cyber actors from threatening the U.S.'s national security or public safety. This pillar will be realized by strategically employing all tools of national power, engaging with the private sector, and addressing ransomware through a comprehensive federal approach in concert with international partners.

3. Shape Market Forces to Drive Security and Resilience

Referencing the global digital ecosystem, this pillar places cybersecurity responsibility on those best positioned to reduce risk. Today, those responsibilities typically fall on organizations and individuals. The focus is on promoting privacy and the security of personal data, shifting liability for software products to promote secure development practices, and ensuring federal grant programs encourage investments in new infrastructure that are secure and resilient.

4. Invest in a Resilient Future

This pillar's goal is innovation in developing secure and resilient next-generation technologies and infrastructure. That includes reducing systemic technical vulnerabilities and increasing resiliency, prioritizing R&D for next-generation technologies like post-quantum encryption, digital identity solutions, and clean energy infrastructure. It also focuses on developing a diverse and robust national cyber workforce.

5. Forge International Partnerships to Pursue Shared Goals

Cybercrime is a global problem, and many of today's enterprises do business worldwide. That's why this last pillar intends to leverage international coalitions and partnerships with other countries to work together on preparedness, response, and how costs are imposed. It includes increasing partners' capabilities to defend against cyber threats and collaborating to make secure, reliable, and trustworthy global supply chains for information technology and operation technology products and services.

Increasing Data Resiliency in Your Business

While this new cybersecurity strategy is national, you can do your part today by strengthening your company's resiliency. That starts with the lifeblood of your business—your data. When it stops flowing, your operation comes to a standstill.

Data resiliency starts with ensuring your disaster recovery plan is continuously updated and regularly tested. As with the national strategy, you must also invest in technologies that protect your data from ransomware and other cyberattacks.

A sound backup and disaster recovery strategy is one of the most crucial components of data resiliency. That starts with a 3-2-1-1 strategy, where you keep three copies of your data (one primary and two backups), with two copies stored locally on two formats (network-attached storage, tape, or local drive) and one copy stored offsite in the cloud or secure storage.

The last "1" stands for immutable storage. When your backups are saved in an immutable, write-once-read-many-times format, they can never be altered or deleted—even by admins. It's your last line of defense against any data loss, whether the cause is ransomware, a cyberattack, or a natural disaster. And it delivers true data resiliency.

Experience and Expertise Matter

Arcserve technology partners bring IT expertise and experience that span businesses of every kind, large and small. They can help you ensure your organization is resilient and ready for anything. Find an Arcserve technology partner here. To learn more about Arcserve products, contact us.

CISA Red Team Cybersecurity Advisory:

Improve Monitoring and Hardening of Networks to Strengthen Data Resilience

The Cybersecurity and Infrastructure Security Agency (CISA) released a lengthy cybersecurity advisory on February 28, 2023; if you have time, it's a compelling read. The advisory takes you through the step-by-step process the CISA Red Team used to emulate cyber threat actors so it can assess an organization's cyber detection and response capabilities.

The reasons for doing so are written in the daily headlines and validated by studies by companies like Check Point Research, which found that cyberattacks were up 38 percent year over year in 2022, and the top five most attacked industries—including communications companies, ISPs, and MSPs—saw about 1380 attacks per week.

Initial Access Relies on the Human Element

For its assessment, the Red Team's "victim" was a large organization with multiple geographically separated sites throughout the U.S. The team aimed to gain access to sensitive business systems (SBSs).

As we've written frequently, the human element is behind many breaches—82 percent— and includes social attacks, errors, and misuse, according to the 2022 Verizon Data Breach Investigations Report. The Red Team's experience was no different, gaining initial access to two of the organization's workstations at separate sites via spear phishing emails that attempt to acquire sensitive information or access a computer system by sending counterfeit messages that appear to be legitimate.

The way the Red Team gained initial access is particularly illuminating, as "the team sent tailored spear-phishing emails to seven targets using commercially available platforms. The team used the logging and tracking features of one of the platforms to analyze the organization's email filtering defenses and confirm the emails had reached the target's inbox."

The attack is a perfect example of social engineering as "the team built a rapport with some targeted individuals through emails, eventually leading these individuals to accept a meeting invite. The meeting invite took them to a red-team-controlled domain with a button, which, when clicked, downloaded a 'malicious' ISO file. After the download, another button appears, which, when clicked, executes the file."

Two of the seven targets responded to the phishing attempt, giving the Red Team all the access it needed to exploit the organization further.

Lateral Movement, Compromised Credentials, and Persistence Pay Off

The advisory continues with an in-depth look at how the Red Team leveraged that initial access to traverse the network and access a SharePoint server. It also explains how the team gained persistent, deep access across the organization's networks and subnetworks.

The advisory notes that "the Red Team executed 13 measurable events designed to provoke a response from the people, processes, and technology defending the organization's network," ranging from data exfiltration to ransomware.

In its findings, the advisory lists these key issues relevant to the security of the organization's network. It's a long list:

- Insufficient host and network monitoring
- Lack of monitoring of endpoint management systems
- The original krbtgt account password had not been changed in over a decade
- Excessive permissions to standard users
- Hosts with Unconstrained Delegation enabled unnecessarily
- Use of non-secure default configurations
- Ineffective separation of privileged accounts
- Lack of server egress control
- Inconsistent host configuration
- Potentially unwanted programs
- Mandatory password changes enabled
- Smart card use was inconsistent across the domain

Mitigations That Worked, But More Are Needed, Including Zero Trust

The team did note that the organization has some technical controls or defensive measures that did work. These included that the organization conducts regular, proactive penetration tests and adversarial assessments. And there were strong security controls and segmentation for SBSs. Also, a multi-factor authentication (MFA) prompt blocked the team from a second SBS.

The advisory, which includes mitigations for each key issue listed above—from improved network monitoring to mandatory password changes—also lists these recommended mitigations to improve your cybersecurity posture:

- Train and test users regularly so they can recognize phishing and other social engineering attacks
- Enforce phishing-resistant MFA to the greatest extent possible
- Reduce credential compromise opportunities

The list goes on but concludes that "as a long-term effort, CISA recommends organizations prioritize implementing a more modern, zero trust network architecture."

Whether you need on-premises immutable network-attached storage like Arcserve OneXafe or support for Amazon S3 Object Lock immutability in the cloud that Arcserve Unified Data Protection (UDP) provides, Arcserve can ensure your data is resilient, and you can recover no matter what.

For expert help improving your cybersecurity posture and data resilience, talk to an Arcserve technology partner. To learn more about Arcserve products, check out our demos on demand.

You'll find the complete CISA advisory here.

Is Your Business in Compliance With Global Data Sovereignty Requirements?

TechTarget defines data sovereignty as "the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located." Compliance with regulations—like the Data Governance Act in Europe—that define the jurisdiction and control of data and how it is stored, used, and protected can present new challenges for companies.

With data a crucial driver for business decision-making and growth and and also with the proliferation of cloud computing, it isn't easy to track where your data is stored and ensure that the data is handled in compliance with local data privacy regulations.

Data sovereignty compliance requires that you follow the local country rules where data is collected. For example, if your United States-based business collects customer data in France, you must comply with the European Union's General Data Protection Regulation (GDPR). If you don't, you could be hit with high costs. In 2022, GDPR fines and penalties for data breaches reached a record €2.92 billion.

For global businesses, maintaining multiple data centers in different countries to ensure compliance with local laws and regulations can be problematic. Here's why:

Cost, Complexity, and Vulnerabilities

The country or jurisdiction where your business is based may not necessarily have sovereignty over all of your data. For example, if you're company is U.S.-based, but you have data stored on servers in the EU, that data is subject to EU data protection laws, not U.S. laws. This makes the point that, when it comes to data sovereignty, the physical location of your data is more important than the location of your business.

You also need to know—and be able to prove—who has access to your data. If your company is keeping your most sensitive information in the cloud, like trade secrets and private customer data, and it gets hacked, it could put your entire organization at risk. Keeping track of who is accessing your data—and when it was accessed—gives you a better shot at preventing unauthorized users from getting in and wreaking havoc.

Backup Implications of Data Sovereignty

With high fines and legal penalties, costs for noncompliance can be steep. That's why you need to ensure your backups are always secure, and you can recover your data if a cyberattack or natural disaster hits you.

You can meet data sovereignty requirements by choosing a cloud services provider (CSP) that ensures compliance with all relevant laws and regulations. Many CSPs offer data centers in different locations worldwide, so you can be confident your data is compliant. The European Commission has advocated for the inclusion of sovereignty provisions by CSPs.

These sovereignty requirements are intended to put data held in the EU out of reach of foreign jurisdictions. That's why you must do your due diligence and select a reputable CSP with a proven track record of compliance with global regulations.

You can ensure compliance by implementing strong data governance policies and procedures. That includes establishing clear rules and guidelines for collecting, storing, and using data and implementing robust security measures to prevent data breaches and unauthorized access to data. You should also consider implementing data masking or encryption techniques to protect sensitive data and ensure compliance.

Getting there demands that you adopt processes and tools that prioritize data protection and go well beyond the basics.

You can also ensure compliance with data sovereignty regulations by adopting transparent data practices. That includes being upfront about where data is stored and how it is used. It also includes being responsive to any inquiries from customers regarding their personal data. This transparency builds trust with your customers and demonstrates your commitment to compliance with data sovereignty requirements.

Final Thoughts

As countries race to put data sovereignty rules in place, the issue of data security and ownership is now front and center. That's why your organization must understand where your data is being stored and who holds the keys to it. This is particularly true when it comes to cloud data.

Get expert help ensuring you comply with data sovereignty requirements by talking to an Arcserve technology partner. To learn more about Arcserve products, contact us.

Researchers Use ChatGPT AI-Powered Malware to Evade Endpoint Detection and Response Filters

ChatGPT is big news these days, and for good reasons. It's the fastest-growing consumer application in history, according to a UBS study, acquiring 100 million monthly users just two months after launching. While it can potentially change our world for the better, it's already become a tool of choice for cybercriminals.

A Bleeping Computer article attributes security researcher Dominic Alvieri as among the first to notice the domain chat-gpt-pc.online. The domain was promoted by a Facebook page featuring official ChatGPT logos and it infects visitors with Redline information-stealing malware disguised as a download for a ChatGPT Windows desktop client. The article notes that Alvieri also saw fake ChatGPT apps promoted on Google Play and other Android app stores.

That's pretty scary. But it gets worse. Traditional security solutions like endpoint detection and response (EDR) rely on multilayer data intelligence systems and automated controls to defend against sophisticated threats today.

Last week, Jeff Sims, a researcher at cybersecurity firm HYAS Labs, posted how his firm was able to generate polymorphic malware courtesy of ChatGPT. HYAS makes a key point: "While EDR and other automated security controls are essential components of a modern security stack, they are not foolproof." This point is underscored by the simple proof of concept (PoC) Sims built to demonstrate what AI-based malware could do.

BlackMamba: Exploiting APIs

Sims' PoC leveraged a large language model—AI software ChatGPT—which uses natural language processing, deep learning, and neural networks to dynamically synthesize polymorphic keylogger functionality. Put more simply, as TechTarget defines it, polymorphic malware uses an encryption key to change its shape and signature, while a keylogger records every stroke of the infected machine's keyboard. It combines a mutation engine with self-propagating code to change its appearance continuously and rapidly morph its code. The result modifies benign code at runtime without running into any command-and-control infrastructure that could stop this malicious threat.

HYAS tested the PoC against an unnamed industry-leading EDR many times. There were zero alerts or detections. HYAS named the PoC “BlackMamba” to convey the seriousness of the threat because this ever-changing malware can evade your EDR defenses.

An executable file was used to deliver the malware. Sims explains that once a device is infected, the PoC employed Microsoft Teams to exfiltrate data, sending it from the compromised system to an external location. HYAS relied on a hacker-controlled Teams channel via webhook, a lightweight API that powers one-way data sharing triggered by events.

The post digs into the technical details of the development and malware delivery process and is worth reading. But the closing paragraph brings it home, stating that “BlackMamba is virtually undetectable by today’s predictive security solutions.”

Employ a Multilayered Approach to Data Resilience

While some hackers go after your people via phishing and other social engineering attacks, plenty of others are testing new ways to use AI to get around your defenses. Fighting back demands constant awareness of changing threats and new defensive strategies.

That’s where Arcserve technology partners make all the difference in the world. They bring expertise, experience, and a dedicated commitment to keeping your data resilient and your business secure. Choose an Arcserve partner here. And be sure to check out on-demand demos.

Need Answers?

Arcserve is always here—standing by and ready to help.

arcserve®

+1 844 639-6792

arcserve.com