**Cybersecurity Threats and Latest Standards: A Guide for Proactive Organizations.**

Cybersecurity threats are constantly evolving. If your organization isn't employing the latest cybersecurity standards, then you're putting your systems at risk.

Don't assume that the standards you implemented two years ago will provide the same protection today. Savvy hacker groups are relentless in finding new vulnerabilities to exploit, effectively making many standards obsolete. Today's organizations must be proactive about identifying these gaps and implementing the latest security protocols and technologies.

Here's a quick look at some of the latest standards to consider, plus the actions being taken at the federal level that businesses can use as a basic guide to identifying the latest threat areas and solutions.

The following standards are comprised of wide-ranging guidelines and best practices for IT and other areas of operations:

* NIST Cybersecurity Framework (CSF) 2.0: This is a voluntary framework provided by the National Institute of Standards & Technology, a division of the Department of Commerce. First published in 2014, CSF provides a comprehensive set of standards for 2mitigating cybersecurity risk, divided into five categories of action: Identify, Protect, Detect, Respond, and Recover. The newest version of the framework, known as CSF 2.0, is scheduled to be published in early 2024.
* ISO/IEC 27001: This is an international standard for IT security management systems. ISO/IEC 27001 was first published in 2005 and most recently updated in 2022. Globally, it is the most widely known standard for managing cybersecurity.
* Service Organization Control Type 2 (SOC 2): This set of compliance standards is primarily geared to third-party service providers that store and manage data for other companies. However, many of the guidelines in SOC 2 are still applicable to most organizations, covering areas including access control, network firewalls, data encryption, and disaster recovery. There are 7 new cybersecurity standards to consider:

**Zero Trust Network Access (ZTNA).**

More organizations are moving away from traditional VPNs to implement more secure Zero Trust Network Access. In the new era of hybrid work, organizations have strengthened their networks to accommodate more off-site workers while also removing vulnerabilities. VPN was the gold standard for off-site access for a while. But it left open too many doors for malicious activity. Generally, once a user is connected to a network via VPN, they gain far-ranging access to that network. With ZTNA, users and devices face a much more granular level of security and access control. Access to network resources and applications is granted only to the specific users and devices that need them.

**Less file Exploit Mitigation.**

Less file attacks occur when vulnerabilities in legitimate systems and software are exploited within a computer's memory (rather than the hard drive). With traditional malware, the infections are delivered via files. With file-less attacks, for example, a user's web browser could be infiltrated simply by visiting a website. When these vulnerabilities are discovered and exploited by attackers before patches are available, they are known as zero-day attacks. The prevalence of file-less and zero-day attacks has required organizations to adopt new cybersecurity standards that mitigate the risks of these threats. Exploit mitigation tools, such as those built into Windows, help to thwart these attacks by detecting the types of techniques commonly used in these attacks. Third-party tools like Sophos Intercept X (an [endpoint detection and response](https://invenioit.com/sophos/sophos-endpoint-protection-pricing/) solution) take this protection even further to prevent users' devices from being exploited, even if vulnerabilities exist.

**Endpoint Security & Backup.**

Building off that last point, a critical cybersecurity standard that today's organizations must implement is endpoint protection. 2 out of 3 companies have experienced "one or more endpoint attacks that successfully compromised data and/or their IT infrastructure," according to Ponemon Institute. And with the increase in hybrid work, workers are now using a greater variety of devices, on different networks, increasing their cybersecurity risks. Stronger endpoint protection is essential to detecting and isolating attacks on the user's device (including mobile devices) before they can spread laterally across a network. Similarly, [endpoint backup](https://invenioit.com/redstor/redstor-servers-endpoints-backup-pricing/) is needed to ensure that files saved locally on users' PCs can be recovered when data loss occurs.

**Security Orchestration, Automation and Response (SOAR).**

The term SOAR was first coined by Gartner in 2015, but it is still a relatively new cybersecurity standard that organizations have adopted over the last few years. In basic terms, SOAR is a software solution that provides an integrated approach to managing diverse cybersecurity tools and tasks. A recent study by IBM found that 52% of large organizations were using between 30 to 100 different security tools and technologies – most of which do not play nicely together. SOAR takes the data from all these tools to create a central console for managing incident response and streamlining security work-flows. More significant security alerts are prioritized, for example, while false positives are automatically filtered out. Result: security is faster, smarter, and more fluid. While SOAR is currently most beneficial to larger organizations, we anticipate that SMB-focused tools will become more ubiquitous in the years ahead.

**Next-Gen Intrusion Prevention Systems (IPS).**

Intrusion prevention systems have long been an effective tool for blocking dangerous network activity. But the next generation of IPS (or NGIPS) is ushering in a new era of smarter threat detection. New IPS technologies allow for a much deeper analysis of network traffic, identifying not just known threats but also contextual data, such as applications, users, files, and so on. This deep analysis is combined with automation to rapidly identify and respond to threats as they happen, across the network. [Firewall solutions](https://invenioit.com/sophos/sophos-firewall-pricing/) from Sophos leverage this next-generation IPS technology and in fact, can be integrated with endpoints and access points for 360-degree protection (what Sophos refers to as Synchronized Security). For example, if a threat is detected on an endpoint, it is immediately blocked and the access point also restricts Internet/network access to the endpoint, so that no further malware can be downloaded or moved laterally.

**AI-Powered Phishing Detection.**

Advancements in AI and machine learning are expected to revolutionize the cybersecurity landscape over the next few years. One area in which AI is already making a big impact is email. New email solutions now use natural language processing (NPL) and machine learning to detect phishing scams and other malicious messages. In the "old days" of spam filtering, messages would be flagged for certain words in an email message, such as "urgent" or "FREE." NPL enables today's cybersecurity systems to understand these words *in context*. This reduces the risk of legitimate emails being flagged as spam and improves the detection of messages from importers. For example, even if the message contains no URLs or malware, [email protection solutions](https://invenioit.com/sophos/sophos-email-protection-pricing/) from Sophos use NPL machine learning to detect and automatically block targeted impersonation and Business Email Compromise attacks. Beyond NPL and email, AI is playing an increasingly important role in all aspects of threat intelligence, using an extensive array of data points to identify potential cybersecurity threats anywhere on the network.

**Managed Detection & Response (MDR).**

[Managed Detection & Response](https://invenioit.com/field-effect-covalence-pricing/) involves having external teams manage a company's cybersecurity. It's not exactly a new concept – various forms of MDR have been available since the early 2000s. However, as evolving threats like ransom ware have become more prevalent and sophisticated, it has become increasingly challenging (and costly) for organizations to manage their security on their own. More companies are now using MDR from providers such as [Sophos](https://invenioit.com/sophos/sophos-mdr-pricing/) to receive round-the-clock threat detection, response, and remediation. MDR thus allows companies to respond to threats much faster and more effectively than they could if they managed their cybersecurity by themselves, significantly reducing the risks and impact of an attack.

## **Revisiting the New Cybersecurity Standards Issued by the U.S. Gov.**

On the federal level, new cybersecurity standards issued by the Biden administration in 2021 continue to reverberate across both the public and private sectors. The elements of the program included:

* The Industrial Control Systems (ICS) Cybersecurity Initiative for Electric Utilities
* Executive Order 14028, Improving the Nation's Cybersecurity
* National Security Memorandum on Defending Against Ransomware
* National Security Memorandum on Improving the Cybersecurity for Critical Infrastructure Control Systems
* The White House Cybersecurity Summit that featured announcements on improving the security of the technology supply chain

Below, we examine the major elements of these five initiatives, review the progress made to date in rolling out these new cybersecurity standards, and describe resources that have been developed to support the moves.

## Electricity Sector Cybersecurity Standard

On April 20, 2021, the Biden Administration launched the [Industrial Control Systems Cybersecurity Initiative](https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0) which is intended to enhance the Nation's cybersecurity of electric utilities' industrial control systems and secure the energy sector supply chain.

The U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) has the leadership role in the program, supported by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). The Electricity Subsector Coordinating Council, which is made up of CEOs and executives from electric companies, public power utilities, and rural electric cooperatives, provides the voice of the electricity industry for the initiative.

The purpose of the undertaking is to advance technologies and systems that will provide cyber visibility, detection, and response capabilities for industrial control systems of electric utilities. Towards this end, the program:

* Encourages owners and operators to implement measures or technology that enhance their detection, mitigation, and forensic capabilities.
* Includes concrete milestones for owners and operators to identify and deploy technologies and systems that enable near real-time situational awareness and response capabilities in critical industrial control systems and operational technology (OT) networks.
* Reinforces and enhances the cybersecurity posture of critical infrastructure information technology (IT) networks.
* Includes a voluntary industry effort to deploy technologies to increase the visibility of threats in ICS and OT systems.

One outcome of the initial 100-day focus was an update to the Department of Energy's [Cybersecurity Capability Maturity Model](https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf) (C2M2). The C2M2 is a self-evaluation methodology and tool that organizations can use to evaluate their cybersecurity capabilities to inform the prioritization of cybersecurity investments.

While developed for the electricity sector, companies in any industry segment can use the framework. It is comparable to the NIST Cybersecurity Framework, but it also includes a maturity measurement technique. The maturity model examines 10 domains, such as threat and vulnerability management, event and incident response, and continuity of operations along a four-point scale of Not Implemented, Partially Implemented, Largely Implemented, or Fully Implemented.

Work already undertaken on the Electricity Sector pilot program has resulted in 150 electricity utilities representing almost 90 million residential customers deploying or agreeing to deploy control system cybersecurity technologies.

## Improving the Nation's Cybersecurity.

President Biden signed Executive Order 14028, [Improving the Nation's Cybersecurity](https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/bidens-executive-order-cybersecurity.html), on May 12, 2021, to improve the nation's cybersecurity and protect federal government networks. While aimed primarily at Federal agencies, the President noted his expectation that these approaches would trickle down to the corporate sector when he said, "We encourage private sector companies to follow the Federal government's lead and take ambitious measures to augment and align cybersecurity investments to minimize future incidents." The major elements of the Executive Order (EO) included:

* Remove barriers to threat information sharing between the government and the private sector by ensuring that IT Service Providers can share information with the government and requiring them to share certain breach information.
* Improve software supply chain security by establishing baseline security standards for the development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available.
* Modernize and implement stronger cybersecurity standards in the federal government by encouraging the movement to cloud services and the deployment of zero trust architecture and mandating the deployment of [multifactor authentication](https://invenioit.com/duo-mfa-pricing/) (MFA) and encryption across the Federal government.
* Improve detection of cybersecurity incidents on federal government networks by enabling government-wide endpoint detection and response (EDR) systems.
* Creating a standard playbook for responding to cyber incidents by establishing a set of definitions for cyber incident response by Federal departments and agencies will also provide a template for private sector response efforts.
* Improve investigative and remediation capabilities through the creation of cybersecurity event log requirements for Federal departments and agencies.
* Establish a Cybersecurity Review Board co-chaired by government and private sector leaders that may convene after significant cyber incidents to analyze what happened similarly to what the National Transportation Board does after airplane crashes.

## Information Sharing.

While most aspects of these initiatives will be carried out through administrative means, it appears that the sharing of ransomware payment and breach information may end up with a legislative mandate. There are competing bills that include 24 or 72-hour reporting requirements, so the exact form, time window for reporting, and companies that will come under the purview of the legislation are still to be resolved as the administration, Congress, and industry trade groups wrangle over the details.

## Software Supply Chain Security.

NIST has fulfilled its assignment under the Executive Order to set up baseline security standards for software development with the publication of two guidance documents: Security Measures for "E0-Critical Software" Use and Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software. The Security Measures document starts with the premise that breaches are going to occur and focuses on monitoring, incident detection, response, and recovery capabilities. The purpose of the Minimum Standards publication is to recommend high-level guidelines for software producers to create their prescriptive processes.

## Zero Trust Architecture Cybersecurity Standard.

In announcing the initiatives related to the EO's zero trust architecture, Chris DeRusha, Federal Chief Information Security Officer, stated, "The Federal government's approach to cybersecurity must rapidly evolve to keep pace with our adversaries and moving toward zero trust principles is the road we need to travel to get there. Today we're releasing a draft federal zero trust strategy that will help agencies put these principles into practice."

Addressing the push to modernize federal government networks through the deployment of zero trust architecture, the Office of Management and Budget released on September 7 a draft memorandum for comment titled, [Moving the U.S. Government Towards Zero Trust Cybersecurity Principles](https://zerotrust.cyber.gov/downloads/Office%20of%20Management%20and%20Budget%20-%20Federal%20Zero%20Trust%20Strategy%20-%20DRAFT%20For%20Public%20Comment%20-%202021-09-07.pdf). The memo requires agencies to achieve specific zero trust security goals by the end of the Fiscal Year (FY) 2024.

Recognizing that most major cyber incidents start with a phishing attack, the memo emphasized the importance of "phishing-resistant approaches" and encouraged the deployment of multi-factor authorization (MFA) solutions, treating internal networks as untrusted and encrypting traffic, and moving protection closer to data by strengthening application security.

## Cloud Services.

To advance the movement to cloud services by Federal agencies, CISA published in August the [Cloud Security Technical Reference Architecture](https://www.cisa.gov/sites/default/files/publications/CISA%20Cloud%20Security%20Technical%20Reference%20Architecture_Version%201.pdf) (TRA). The document offers recommended approaches to cloud migration and data protection. The publication explains considerations for shared services and cloud security posture management.

Complementing the TRA document is the [Zero Security Maturity Model](https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf). While the TRA focuses on technical implementation and security issues, the Maturity Model supplies a roadmap for achieving an optimal zero-trust environment and a means of measuring progress toward this goal. The model is built upon five pillars: Identity, Device, Network, Application Workload, and Data, which are assessed as falling into one of the stages of development: Traditional, Advanced, or Optimal.

Recognizing that much work has to be done by federal agencies, Jen Easterly, head of CISA commented about the new model, "We know that it is a journey. Some organizations are just on the front end of re-architecting their networks, so we wanted to give them benchmarks to get to, in how they advance in maturity."

## EDR.

On October 8, 2021, Shelanda D. Young, Acting Head of the Office of Management and Budget, issued a memorandum in support of the EO to agency heads directing them to move cyber defense from a reactive to a proactive posture by [adopting robust EDR solutions](https://cpl.thalesgroup.com/data-protection/executive-order-to-strengthen-cyber-security).

The memo offers implementation guidance and timelines to deliver on commitments to improve visibility into and detection of cybersecurity vulnerabilities and threats, particularly malware, advanced persistent threats, and phishing.

## Defending Against Ransomware.

The Ransomware Memorandum issued by Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technologies, is the one item among these five initiatives directed solely to the private sector. She addressed the memo to corporate executives with the subject line: "What We Urge You to Do to Protect Against the Threat of Ransomware." The memo highlighted the responsibility the private sector has in complementing the programs being undertaken by the Federal government to disrupt and deter ransomware actors.

She outlined the U.S. government's recommended best practices that can have the most impactful short-term effect. The memo counsels all private sector entities to:

* Implement the five best practices from the President's Executive Order (MFA, EDR, encryption, an empowered security team, and threat information sharing).
* [Back up your data, system images, and configurations](https://invenioit.com/datto-backup/datto-siris-5-pricing/), regularly test them and keep the backups offline.
* Update and patch systems promptly, including operating systems, applications, and firmware.
* Test your incident response plan including a focus on the interaction of IT and OT systems/ICS networks.
* Check your security team's work using a 3rd party penetration tester.
* Segment your networks so corporate business functions and manufacturing/production operations so that ICS networks can continue operating if your corporate network is compromised.

Not long after the release of the ransomware memo, the Justice Department announced the launch of a one-stop ransomware resource at [StopRansomware.gov](https://www.cisa.gov/stopransomware). This site represents an effort to overcome the previous fragmentation of ransomware information by consolidating resources from all federal agencies, including alerts and updates. The platform also supplies victims of cyber incidents with clear guidance on how to report attacks.

## Improving Cybersecurity for Critical Infrastructure Control Systems.

President Biden signed the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems on June 28, 2021. This memo builds on the Electricity Sector ICS program launched in April by formalizing the program and creating the structure to eventually expand the methodology to all major critical infrastructure sectors.

Characteristic of the administration's approach of mixing cooperative efforts and required actions, the White House stated, "Given the evolving threat we face today, we must consider new approaches, both voluntary and mandatory. We look to responsible critical infrastructure owners and operators to follow voluntary guidance as well as mandatory requirements to ensure that the critical services the American people rely on are protected from cyber threats."

The initiative calls on the industry to deploy systems and technologies that can monitor control systems to detect malicious activity and facilitate responses to cyber threats and asks Federal agencies and companies to share threat information for priority control system critical infrastructure throughout the country. The program was expanded to include the Natural Gas Pipelines Sector with plans to add the Water and Wastewater System and Chemical Sectors by the end of this year.

The other component of the memorandum directs CISA and NIST to lead the development of cybersecurity standards and performance goals for critical infrastructure. On September 23, NIST released a preliminary set of performance goals and objectives. The two agencies identified nine categories of cybersecurity practices that support the deployment and operation of secure control systems with each category having a set of baseline and enhanced objectives. The categories are:

* Risk Management and Cybersecurity Governance
* Architecture and Design
* Configuration and Change Management
* Physical Security
* System and Data Integrity, Availability, and Confidentiality
* Continuous Monitoring and Vulnerability Management
* Training and Awareness
* Incident Response and Recovery
* Supply Chain Risk Management

## Technology Supply Chain.

On August 25, President Biden hosted a White House Cybersecurity Summit that included private sector and education leaders and resulted in several initiatives and commitments including:

* A Federal government/private sector collaborative effort to develop a framework to improve the security and integrity of the technology supply chain. The initiative is tasked with developing guidelines on how to build secure technology and assessing the security of technology. NIST will lead the initiative with participation from Microsoft, Google, IBM, Travelers, and Coalition (a cyber insurer).
* An announcement by Apple that it will establish a new program to drive continuous security improvements throughout the technology supply chain including mass adoption of multi-factor authentication, security training, vulnerability remediation, event logging, and incident response.
* An announcement by Google that it will invest $10 billion over the next five years to expand zero trust programs, help secure the software supply chain, and enhance open-source security.

NIST is working on a new framework for securing the technology supply chain and is [developing an RFI to solicit input](https://federalnewsnetwork.com/cybersecurity/2021/10/nist-seeks-feedback-on-potential-moonshot-of-supply-chain-security-project/) from the industry to define principles to structure the program and to address the issue of the sharing of sensitive supply chain security information with a Federal agency. As Jon Boyens, the Deputy Chief of NIST's Computer Security Division put it, "One of our big questions I think we'll put in the RFI is how to get a trust mechanism similar to what we're doing in the software world: artifacts, evidence to achieve greater trust, to achieve greater assurance in the supply chain without sacrificing intellectual property."

## Conclusion.

As threats continue to evolve, organizations must be proactive about adopting new cybersecurity standards to protect their systems from being compromised. The latest solutions for protecting endpoints, email, networks, and data are significantly better at thwarting attacks, especially when implemented properly as part of an integrated cybersecurity and business continuity strategy. On a federal level, the government has also created a comprehensive and long-term vision for a proactive cybersecurity posture for the public and private sectors. Organizations that take advantage of the frameworks, practices, and technologies proposed in these new cybersecurity standards can significantly enhance the resilience of their businesses.

**Reference**

**Author, Dale Shulmistra.(January 20th 2024). New cybersecurities standards for 2024**

**https://www.riskandresiliencehub.com**