ExtraHop

SHIELDS UP

A Practical Guide For Shields Up

Advice for Corporate Leaders and CEOs in Implementing CISA's Cybersecurity Doctrine to Defend your Enterprise

Executive Summary

Since its inception in 2018, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) has worked to provide critical guidance and information to government and private sector organizations about critical cyber threats. In response to the Russia-Ukraine conflict, CISA issued its first-ever *Shields Up* notice, warning that with its cyber capabilities and history of targeting Western governments and corporations, cyberattacks from Russia are likely, if not imminent. In this notice, CISA provides guidance for organizations, corporate leaders and CEOs, and individuals around how best to prepare for and defend against this attack activity. In this white paper, we walk through the CISA guidance for corporate leaders and CEOs and provide recommendations for implementation and maturation.

Introduction

On February 25, 2022, two days after Russia began its military invasion of Ukraine, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) issued a rare *Shields Up* warning for U.S.-based organizations, stating: "Every organization—large and small—must be prepared to respond to disruptive cyber activity."

The *Shields Up* warning was in direct response to increased Russian cyber aggression against Ukrainian and other targets in the region, including a spate of distributed denial-of-service (DDoS) and malware attacks. In addition to the possibility of disruptive nation-state activities affecting U.S. targets, CISA also warned of an increase in ransomware activity seeking to take advantage of the geopolitical disruption.

CISA *Shields Up* guidance was comprehensive in its scope, making recommendations targeted at security organizations, corporate leaders and CEOs, and individual consumers. In this white paper, we break down the CISA guidance and provide concrete recommendations about how corporate leaders can implement this guidance quickly and comprehensively.

What is CISA and Why Does It Matter?

The Cybersecurity and Infrastructure Security Agency "leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure." The organization, part of the Department of Homeland Security, works to connect stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people.

Created in 2018, CISA is now the operational lead for all federal cybersecurity. The agency issues requirements and guidance for federal agencies and contractors, as well as private-sector organizations and state and local governments. Over the past twelve months, CISA has had many occasions on which to do this. In 2021, the agency issued two dozen alerts covering everything from ransomware attacks like that on Colonial Pipeline, to urgent advisories around ProxyShell and Log4j, to guidance on Russian Foreign Intelligence Service cyber operations.

CISAs alerts, and the guidance the agency offers alongside them, help organizations identify and prioritize the most pressing cybersecurity threats. It also helps security leaders effectively communicate these priorities to the broader organization.

What is Shields Up?

The *Shields Up* warning issued by CISA is the first of its kind, and provides sweeping guidance for security organizations, business leaders, and individuals. While the notice acknowledges that there are "no specific or credible cyber threats to the U.S. homeland at this time," it warns that, in light of unprovoked Russian aggression against Ukraine, the cybersecurity impacts may extend beyond the region of conflict.

The CISA *Shields Up* guidance for corporate leaders and CEOs falls into five broad categories.

1. **Empower Chief Information Security Officers (CISO)**
2. **Lower Reporting Thresholds**
3. **Participate in a Test of Response Plans**
4. **Focus on Continuity**
5. **Plan for the Worst**

We will discuss each of these five categories with concrete steps leaders can take to strengthen organizational resilience. For more information about *Shields Up* guidance for organizations, visit www.cisa.gov and check out the ExtraHop whitepaper: "A Practical Guide for Shields Up: Advice for Organizations in Implementing CISA's Cybersecurity Doctrine to Defend Your Enterprise."

Implementing Guidance and Recommendations for Corporate Leaders and CEOs

This section details the five key recommendations for corporate leaders and CEOs outlined in the CISA *Shields Up* warning, and provides specific implementation and maturation guidance on each element of those recommendations.

For CISA's guidance for security organizations and associated implementation recommendations, click here.

1. Empower Chief Information Security Officers (CISO)

CISA Guidance: *In nearly every organization, security improvements are weighed against cost and operational risks to the business. In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company, and ensure that the entire organization understands that security investments are a top priority in the immediate term.*

Implementation and Maturation Recommendations: While most stakeholders agree that cybersecurity is a top priority, the friction introduced by many security tools and processes has proven to be a barrier to widespread adoption for many organizations. During a time of "high alert" it's important to assess risk, security posture, and recalibrate the tradeoffs between security and business. ExtraHop recommends taking the following steps to assess your risk:

- Conduct a full risk assessment of all IT and OT assets to determine the level of risk that the CISO is accountable for, including the risk of data loss and non-compliance.
- Document and identify all threats, including nation states, criminal, and ideological, that could act against the enterprise.
- Determine the most appropriate cybersecurity frameworks and compliance frameworks for which the CISO is accountable.
- Ensure adequate resources are provided to the CISO, equitable to address the risks and threats facing the enterprise.

The good news is that, as cybersecurity has grown more sophisticated, many of the traditional points of friction, including device-level instrumentation and cumbersome user authentication, have been substantially reduced. The ability to detect and investigate threat activity in communications across all networks—both on-premises and cloud—has also helped to ease the friction by lessening the reliance on more cumbersome security tools.

During or in the immediate aftermath of an attack, corporate leaders and CEOs also need to carefully consider how they communicate with a CISO and his or her team. Understandably, business stakeholders are often hungry for information in order to manage their own crisis response. However, in the hours and days after an attack has come to light, the

CISOs most important job is incident response and investigation. Determine an appropriate update cadence in advance that will satisfy the information requirements of all parties while also allowing the CISO and security operations teams to remediate the incident as quickly as possible.

2. Lower Reporting Thresholds

CISA Guidance: *Every organization should have documented thresholds for reporting potential cyber incidents to senior management and to the U.S. government. In this heightened threat environment, these thresholds should be significantly lower than normal. Senior management should establish an expectation that any indications of malicious cyber activity, even if blocked by security controls, should be reported, as noted in the Shields-Up website, to CISA or the FBI. Lowering thresholds will ensure we are able to immediately identify an issue and help protect against further attack or victims.*

Implementation and Maturation Recommendations: Most organizations today are subject to some reporting requirements from regulatory frameworks including GDPR, HIPAA, PCI, and CCP. Additional reporting requirements are likely, including disclosures related to ransom payments (Ransom Disclosure Act). During times of heightened threat activity, reporting attacks to the appropriate government agencies can aid these agencies in providing guidance to other organizations, protecting consumers, and helping to thwart future attacks. ExtraHop recommends the following incident-reporting best practices:

- Document both internal and external reporting thresholds based on threat levels, threat actors, compliance requirements, and enterprise risks. Translate those thresholds into graduated reporting groups, based on total risk level with a decision control gate for each risk level that determines follow-up actions and external notifications. Have those decision control gates approved by both legal and public relations teams.
- Begin a dialogue with your local federal law enforcement cyber agency, specifically the local FBI's InfraGard coordinator, FBI's cyber program human intelligence agent, or FBI cyber program coordinator.
- Join multiple threat forums, including your industry ISAC, FBI InfraGard, and SANS.
- Err on the side of caution in reporting to federal law enforcement; it is better to over report than under report.
- Leverage multiple data sources including network intelligence as part of a comprehensive incident response strategy to accelerate the identification of all compromised systems. This not only helps ensure compliance, it also can help avert a broader business disruption.

3. Participate in a Test of Response Plans

CISA Guidance: *Cyber incident response plans should include not only your security and IT teams, but also senior business leadership and Board members. If you've not already done so, senior management should participate in a tabletop exercise to ensure familiarity with how your organization will manage a major cyber incident, to not only your company but also companies within your supply chain.*

Implementation and Maturation Recommendations: Tabletop exercises are an important mechanism for determining organizational response readiness for a cyber incident. ExtraHop recommends taking the following steps in advance of performing a tabletop exercise:

- Designate a crisis response team that will serve as the front line in coordinating the organization's response strategy. In addition to front-line security responders, crisis response teams should also include IT Operations, DevOps, legal, and communications personnel.
- Determine who will be responsible for communicating with key constituencies including shareholders, customers, and employees.
- Develop an organizational continuity of business operations plan (BCP).
- Develop a crisis management and communications plan (CMCP).
- Develop a disaster recovery plan for critical technologies and production capabilities (DRP).
- Develop an incident response plan for responding to cybersecurity incidents (IRP). Use NIST SP 800 61R2 as a guide. Document lessons learned from the tabletop exercises, and use those to improve your IRPs and other contingency plans, as well as incorporate internal and external stakeholders (such as incident response teams and outside counsel) into crisis plans.

4. Focus on Continuity

CISA Guidance: *Recognizing finite resources, investments in security and resilience should be focused on those systems supporting critical business functions. Senior management should ensure that such systems have been identified and that continuity tests have been conducted to ensure that critical business functions can remain available subsequent to a cyber intrusion.*

Implementation and Maturation Recommendations: As a general prerequisite to all IRPs, DRPs, and BCPs, conduct a business impact analysis (BIA). A business impact analysis will help you determine your most critical business and operational systems. Conduct a formal BIA in accordance with guidance in NIST SP 800 34R1 and SP 800 53R5, using the BIA Template.

Based on the BIA, ensure that adequate protective resources, compensating controls, redundant systems, and backup recovery controls are implemented to support the resilience of the critical systems. Use the NIST SP 800 34R1 Guides for Low Impact, Moderate Impact, and High Impact Systems. Determine the senior leadership responsible for the critical business systems, and hold them accountable for resilience controls for their critical systems.

5. Plan for the Worst

CISA Guidance: *While the U.S. government does not have credible information regarding specific threats to the U.S. homeland, organizations should plan for a worst-case scenario. Senior management should ensure that exigent measures can be taken to protect your organization's most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary.*

Implementation and Maturation Recommendations: Until very recently, the most advanced attack techniques, including software supply chain compromise and the use of zero day, was confined to nation-state actors. Russia has long been a major player in the cyber landscape, with a number of highly sophisticated and damaging attacks including NotPetya, which was attributed to Russian advanced persistent threat (APT) groups. While U.S. intelligence agencies have not warned of an imminent threat, the past is a good indication of what the near future may hold. ExtraHop recommends the following "prepare for the worst" strategies:

- Understand the situation with escalating tensions in Ukraine and with NATO, including how it can impact your organization as part of one or more critical infrastructure as a potential target. Become a part of your industry's ISAC to stay informed of critical infrastructure-specific threats.
- Communicate your business continuity plan and/or your continuity of business operations plan to all of your employees.
- Understand that acts of war are generally an exclusion for most cybersecurity breach intrusion insurance policies. There is no ability to transfer risk using cyber insurance. Risk must either be remediated (i.e. fixed and removed), or mitigated (i.e. managed through compensating controls).
- Segment your network and restrict access to and from the internet and mobile devices, as a compensating control against potential cyberattacks.
- Implement continuous monitoring for behavioral anomalies taking place on your network, or work with a third party, such as a managed service provider, to perform this monitoring.

The Foundations of Information, Network, and Cloud Security

The CISA Shields Up guidance provides an important road map for hardening an organization's infrastructure in times of crisis. An organization's cybersecurity maturity, access to resources, and support from corporate leaders, all affect the ease of implementing those recommendations. ExtraHop recommends the following ten areas of focus to mature cybersecurity postures to prepare for future threats.

1. Determine Your Risk Management Strategy

An enterprise risk management strategy is the process of identifying and understanding what your risks are and how much those risks could cost your enterprise. Identify the sources of risk, including people, processes, technology, and infrastructure, and assess the associated financial, operational, and reputational fallout.

2. Determine Your Most Appropriate Technical Cybersecurity Framework

Robust technical frameworks include the NIST Cybersecurity Framework (CSF), Center for Internet Security (CIS) Top 18 Critical Security Controls, ISO 27001/2, or NIST SP 800 53R5. Note that cybersecurity frameworks should be implemented in addition to any regulatory compliance frameworks, as regulatory compliance is not equal to effective cybersecurity.

3. Get Executive Stakeholder Support

To obtain the operational and technical resources necessary to minimize risks and implement your chosen cybersecurity framework, it's important to gain executive stakeholder support from the CEO, COO, CCO, and CFO. Security leaders can leverage CISA and other guidance to help effectively communicate with these stakeholders about risks and priorities. Security leaders should also work with corporate leaders to plan for communications in the event of a breach.

4. Maintain an Inventory of Your Assets

Asset management is the process of identifying, documenting, and continuously maintaining an accurate inventory of devices, applications, cloud assets (SaaS, IaaS, and PaaS), user accounts, and vendors. This process is a critical step toward knowing what is connected to your environment, and who has access. Asset management lays the groundwork for effective mitigation of vulnerabilities, identifying and remediating any insecure protocols, and detecting unauthorized user access.

5. Manage Your Access Controls

Stolen credentials from phishing and brute force are a common way for attackers to gain access to your data. To help prevent this, your organization should effectively provision and carefully manage who has access to your environment. Know who your users are, including administrative, elevated privilege, general, and third-party vendors who may require access to your environment.

6. Reduce Your Attack Surface

Reduce your attack surface by managing your environment. Implement effective change management, configuration management, and patch management to reduce misconfiguration errors. Reduce end of life and end of service (EOL/EOS) vulnerabilities for necessary applications by implementing compensating controls.

Reduce overall vulnerabilities by implementing an effective vulnerability management program that includes periodic scanning, tracking, and escalation of externally facing or critical/high vulnerabilities.

7. Maximize Your Visibility

To help detect threats and stop threats at endpoints and post-compromise, maximize your organization's visibility of the technical operating environment through effective detection tools. These should include network detection and response (NDR), endpoint detection and response (EDR), and security information and event management (SIEM).

8. Monitor Unexpected and Unusual Behavior

Unusual behavior can take many forms, and can originate from any software. SolarWinds SUNBURST is an excellent illustration of how attackers used notoriously "noisy" software to obscure unusual behavior. Monitor for attack techniques that exploit public facing applications, connect to external remote services, use brute force to gain access, or exploit credential access or command and control. Both device-level monitoring as well as cross-network monitoring should be used to identify patterns of potential threat activity.

9. Identify and Cover the Gaps

Ensure you have a complete picture of your security posture, including unmanaged devices (such as IoT) and areas where logging is not possible (such as DNS). While instrumenting devices through logging and agents is best practice, many organizations lack much-needed visibility from network traffic to inventory unknown assets, unmanaged devices, and devices that cannot be instrumented. This approach can also help ensure the security of cloud workloads.

10. Plan for and Prepare for Critical Incidents

Planning and training for critical incidents includes disaster recovery and incident response. Preparation also includes ensuring that your company has frequent backups that are usable, accurate, and safely maintained.

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

ExtraHop

info@extrahop.com
www.extrahop.com