CSDE
Council to Secure the Digital Economy

CYBER CRISIS RESPONSE AND HANDLING

A CYBER CRISIS, where important or critical national infrastructure assets are impacted by malicious actors, is a real possibility. The information and communications technology (ICT) sector's readiness, speed and capabilities for responding to such a crisis will be paramount.

What Keeps Us Up at Night?

- Not all threats or crises are created equal. In recent years, we have seen cyber-attacks against power plants, oil and gas companies, financial centers, military organizations, hospitals, governments, and virtually every other sector that supports modern civilization. Threat actors are continuing to evolve their techniques, tactics, and procedures (TTPs). Response, too, must evolve to meet this challenging landscape.
- The recent Log4j vulnerability has triggered the highest levels of concern because it could turn into exactly the type of infrastructure attack addressed here. Infrastructure providers have not—as of this writing—reported crippling attacks. However, the pervasiveness of Log4j, the likelihood of injected malware in affected systems, and the many reports of malicious scans indicates the strongest and most urgent action is required, as CISA warned in a broad industry briefing on December 13th 2021.
- Below, we provide insights from CSDE's Cyber Crisis Report (available at CSDE.org), which was created to deal with exactly these and other types of urgent situations.[1]

Who You Gonna Call?

- Response is critical; and it's also critical to model the preparation and quick action characteristic of great response.
- Different approaches for response can emerge or be leveraged across the ICT sector. Response to confirmed incidents with wide evidence for exploitation differs from processes for vulnerability handling aimed at developing and releasing a remediation. Vulnerability remediation aims to reduce the risk of a vulnerability being operationalized by a threat actor or exploitation—overall reducing the risk of a future crisis. When confronting vulnerabilities like Log4j, where disclosure occurs prior to remediations being widely available, given information on active exploitation, these processes may converge.
- While many threats are mitigated successfully by individual companies, more complex or significant threats—with broad impact on multiple parts of ICT supply chain and sectors of society—require coordination among multiple ICT companies. Vulnerability handling, where a security risk is remediated to reduce risk for an incident or exploitation resulting in a crisis, may also require coordination among multiple parties. The Log4j vulnerability exemplifies the type of vulnerability where many stakeholders across the ecosystem are at risk, and the incident is being coordinated between multiple parties and coordinators.

1 https://csde.org/wp-content/uploads/2019/09/CSDE_CyberCrisis-Report_2019-FINAL.pdf.

- The major ICT companies handle and combat the increasingly sophisticated and emerging cyber threats of all types through their collaborative actions. Many of these leaders and innovators make up the Council to Secure the Digital Economy: Akamai, AT&T, Cisco, Ericsson, IBM, Intel, Lumen, NEC, NTT, Oracle, Panasonic, Samsung, SAP, Telefónica, and Verizon.
- These leaders also contribute to the development of best practices and standards in this space, and foster the operational collaboration and partnership needed for effective cyber response across industry, governments, coordinators and the security and research community. Consistent with the findings of the CSDE report, CISA, through the Joint Cyber Defense Collaborative (JCDC) is working closely with public and private sector partners to proactively address the vulnerability affecting products containing the Log4j software library.
- Each company has unique expertise and takes substantial steps to protect important systems and services that people, enterprises, and governments depend upon. Many other organizations enable crisis response and members of CSDE facilitate working relationships and processes needed to effectively respond to emerging issues.
- CSDE members and their partners routinely build capacity and "muscle memory" through crisis management planning and other preparedness efforts that help us scale our efforts for many forms or type of incidents, threats or vulnerabilities.

Roles in Cyber Crisis Response and Handling

- As a major voice of global ICT companies, CSDE promotes tools for collaboration among industry and government to prepare for and mitigate potential cyber crises—including actual incidents and significant vulnerabilities.
- CSDE's Cyber Crisis Report (available at CSDE.org) provides a blueprint for how companies can coordinate in 12 different types of crises or events—based on real world scenarios. The report has been widely circulated in policy circles and informed the work of key government partners.
- CSDE initially explored the following initial set of scenarios where cooperation among multiple companies is key to address the risk, addressing various types of events—attacks, incidents, or vulnerabilities. Log4j would fall under the categories of Software Vulnerability: Open Source and Software Vulnerability: Zero Day.
  - *DDoS Botnet Attack*
  - *DDoS Server-based Attack*
  - *Border Gateway Protocol (BGP) Hijacking*
  - *Domain Name System (DNS) Hijacking*
  - *Software Vulnerabilities: Open Source*
  - *Software Vulnerabilities: Zero Day*
  - *Hardware Vulnerabilities: Processor Architectures*
  - *Injection of Malicious Code in Software and Hardware Components*
  - *Destructive Malware*
  - *Ransomware*
  - *Advanced Persistent Threat (APT): Industrial Systems*
  - *Cloud Provider Compromise*

Key Insights

- Organizations must collaborate within their own sectors, the ecosystem at large and with governments to share knowledge of pertinent cyber threats and confirmed incidents. Information sharing and operational collaboration is key, and may differ based on the incident or threat. Indeed, enterprises are often the first to discover a cyber threat because their systems are directly impacted when an incident occurs.
- Government should build close working relationships with the companies whose leadership and experience in responding to major cyber incidents makes them valuable partners.
- When vulnerabilities are discovered, organizations collaborate to validate the vulnerability, develop a remediation, test it in various environments and coordinate the public release of the remediation in a manner that increases its adoption.
- These coordinated vulnerability disclosure and handing (CVD) processes may include multiple parties given the ecosystem collaboration needed for effective remediation. Information about the vulnerability is kept in confidence and shared only with parties necessary to the process, until a remediation is available **and publicly released**. The purpose of CVD processes is to reduce the risk of a potential exploitation of the vulnerability or threat (or threat maturing or enabling an incident) by providing effective remediation. Vulnerabilities differ at their risk and security level.
- Industry must be prepared to mobilize rapidly and to collaborate with relevant responders. This industry-led response should be based on voluntary frameworks and informed by international standards and industry best practices.
- Increasingly, policymakers recognize the need for international cooperation and coordination to address the growing epidemic of cyber-attacks.