CISO board brief: *critical vulnerability*

Two pages from the CISO to the board. **The first within hours of disclosure, the rest at the times the incident response procedures set.** Fill in the middle column. The right column is what a good answer looks like. Page two can follow in a later brief.

VULNERABILITY AND CVE	BRIEF NO.	DATE AND TIME	NEXT BRIEF DUE	PREPARED BY (CISO)

Within hours

The board gets these first.

ACCOUNTABLE OWNER	THE PLAN, AND WHEN EACH STEP ENDS	EXPOSURE IN DOLLARS

One name, with authority to act. A dollar range is fine in the first brief: say what moves it, and narrow it in each brief after that.

Exposure window

Compare the last two.

FIRST PUBLIC SIGNAL	HOURS TO PRODUCE THE FULL LIST	EXTERNAL DEADLINE, AND WHO SET IT	OUR TIME TO PATCH OR ISOLATE

For PHP2Shell, the first public signal was the October 20 leak. CISA listed both CVEs as known exploited on October 26 and set US federal agencies a due date of October 29, 2026, under BOD 26-04.

QUESTION	REPORT	A GOOD ANSWER
1 **Affected systems** How many affected systems exist, and where?		A count from the asset and software inventory, not from memory. Internet-facing systems listed first, each with its version and owner. CIS SAFEGUARDS 1.1 · 2.1
2 **Inventory** How is the inventory kept current, and how complete is it?		Names how assets are discovered and when the inventory was last reconciled. Says what it cannot see: the software inside vendor appliances, the systems nobody owns. CIS CONTROLS 1 AND 2
3 **Patched** What is patched?		Patched and remaining counts by priority, internet-facing and high-risk systems first, with the date the rest will be done. CIS SAFEGUARDS 7.3 · 7.4
4 **Not patched** What cannot be patched, and what protects it until it can?		Every system on the exception register with an owner, a migration date and a compensating control. A WAF rule or other virtual patch counts only if it has an expiry date. CIS SAFEGUARD 2.2
5 **Offline** What was taken offline, and who decided?		The systems isolated or taken offline, the person who decided under written authority, and the business impact so far. CIS SAFEGUARDS 12.2 · 13.10 · CONTROL 17
6 **Board decision** What does the board need to decide?		Any vulnerable system the business wants kept online, with the business owner's signature on the exception and its residual risk. "None" is a valid answer.

THREE QUESTIONS TO ASK BEFORE THE NEXT ONE

1. Show me the inventory, and how do we know it is complete?
2. What on that list cannot be patched, and what protects it until it can?
3. Who can take a system offline in an emergency, and who can overrule them?

Built from the PHP2Shell week (CVE-2026-109618 and CVE-2026-109619, October 2026). Full article: fredriklindstrom.info/articles/php2shell-inventory-board-questions/ · Safeguard references: CIS Critical Security Controls v8.1 (June 2024).

FOLLOW FREDRIK LINDSTROM FOR MORE

Fredrik Lindstrom

AI and cybersecurity governance for boards, CISOs and senior leaders. 25+ years in enterprise security.

A practitioner to guide you.

ARTICLES & BOARD ADVISORY
fredriklindstrom.info
Long-form governance analysis and toolkits

LINKEDIN
in/fredriklindstrom
Daily commentary and article launches

YOUTUBE
@Promise-and-Risk-AI
AI education without the hype or fear

COMPANION SITE
promiseandrisk.ai
Episode notes, sources and explainers

NEWSLETTER
The Governance Memo
Monthly, board-facing. Subscribe at fredriklindstrom.info

CISO board brief: *critical vulnerability*

VULNERABILITY AND CVE

BRIEF NO.

DATE AND TIME

7 Before we patched

What happened between first exploitation and the patch, and who checked?

AFFECTED SYSTEM	EXPOSED FROM	PATCHED OR ISOLATED	HUNT RUN: BY WHOM, WHAT SCOPE	RESULT

> "No alerts" is not evidence of no compromise. Any system exposed during active exploitation gets a hunt before anyone calls it clean.

Each exposed system listed with its window measured from the earliest credible exploitation date, not the patch date. A named team ran the hunt, with its scope written down, in logs that covered the window. For PHP2Shell the window opens on October 17, four days before the fix.

CIS CONTROLS 8 · 13 · 17 · SAFEGUARD 8.2

8 Connected equipment outside IT

Does the inventory cover what facilities, operations and contractors run, and who can reach it?

EQUIPMENT CLASS	BUSINESS OWNER	ON THE ASSET INVENTORY	REACHABLE FROM THE INTERNET	WHO REACHES IT REMOTELY, THROUGH WHICH SUPPLIER	SUPPORTED OR END-OF-LIFE	OPERATIONS CONTINUE IF IT IS OFFLINE?
Refrigeration and cold chain		Yes · Partly · No	Yes · No · Unknown			
HVAC and building management		Yes · Partly · No	Yes · No · Unknown			
Physical access control		Yes · Partly · No	Yes · No · Unknown			
Production or warehouse controllers		Yes · Partly · No	Yes · No · Unknown			
		Yes · Partly · No	Yes · No · Unknown			

> Equipment that can be reached remotely is part of the attack surface, whoever paid for it. A supplier's remote-access path into it is our risk as well as the supplier's.

Every class has a business owner and an inventory entry; CIS Control 1 counts IoT and non-computing devices as enterprise assets. Each remote path is named by supplier and sits behind MFA. End-of-life firmware goes on the Safeguard 2.2 exception register with page one's software.

CIS CONTROLS 1 · 12 · 15 · SAFEGUARDS 6.4 · 15.4

Trigger. A successful attack on a peer, on a product class we may run, starts the same clock as a critical CVE, even when no CVE exists.

Example. October 2026: attackers remotely defrosted refrigeration in hundreds of French supermarkets through internet-reachable controllers, many of them older units no longer receiving updates.

9 What changes after this one

What do we change in our own targets and in our suppliers' contracts?

Critical patch SLA
Internet-facing systems

Target _____ hours Actual, this event _____ hours

A target in hours, set before the event, and the actual against it.

CIS SAFEGUARD 7.2

Supplier contracts
Products, managed equipment or remote access involved

Suppliers _____

Time-to-patch clause Yes · No Right to know who has remote access Yes · No

Each supplier has a contracted time to patch and a duty to say who has remote access. Where the contract is silent, the renewal date that fixes it.

CIS SAFEGUARD 15.4

THREE MORE QUESTIONS FOR THE NEXT ONE

1. What happened on our exposed systems before the patch, and who checked?
2. What do facilities and our contractors run that IT cannot see?
3. Which supplier contracts let us demand a patch, or know who has remote access?

Example: CERT-FR alert CERTFR-2026-ALE-012 (October 12, 2026) and Danfoss via Reuters (October 13, 2026). Deadline: CISA Known Exploited Vulnerabilities catalog and BOD 26-04. Full article: fredriklindstrom.info/articles/php2shell-inventory-board-questions/ · Safeguard references: CIS Critical Security Controls v8.1 (June 2024).

FREDRIK LINDSTROM
fredriklindstrom.info

A practitioner to guide you.