RED ALERT



DO THE CYBER SECURITY BASICS.

Before it becomes an operational crisis.

A five-page brief for boards, CEOs, CIOs and CISOs to ask the hard question — are we actually ready? Not with policies. With dates, evidence and decisions.

Charles Aunger, MSc FBCS
Global Technologist. Futurist. Operator.

CHARLESAUNGER.COM

FOR THE BOARD AND C-SUITE

ASK YOUR CIO AND CISO

Are We *Good?*



It is the only question a board really wants answered. Ask these seven questions this month. **If the answer is a policy, not a date, you have your answer.**

DO IT NOW

01 **When did we last restore a critical system from backup, and how long did it take?**

REAL ANSWER: A recent date and a number of hours.
RED FLAG: Our backups run every night.

02 **What can an attacker see from the internet, right now?**

REAL ANSWER: A current list, checked this month.
RED FLAG: We passed a pen test last year.

03 **How fast do critical patches reach every system, including devices?**

REAL ANSWER: A number of days, with exceptions owned.
RED FLAG: Most systems are patched.

THIS MONTH

04 **Who holds admin rights today, and when did we last take some away?**

REAL ANSWER: A number, a date, and accounts removed.
RED FLAG: Only IT has admin access.

05 **If email, chat and phones were gone tomorrow, who decides and how do we reach each other?**

REAL ANSWER: A named person and an offline list, rehearsed.
RED FLAG: It's in the incident response plan.

THIS QUARTER

06 **When did we last rehearse recovery for real, and what broke?**

REAL ANSWER: A date and what failed and was fixed.
RED FLAG: We ran a tabletop.

07 **Which outside parties connect into our network, and who owns each connection?**

REAL ANSWER: A list with an owner against every line.
RED FLAG: Our vendors are responsible.

"Attackers test what you do, not what you wrote down."

Ask again in three months and expect better dates each time.



WHAT TO DO FIRST

Your First 30 Days.

Start with actions that reduce exposure and prove recovery. Work left to right.
Week 1 is not optional.

Week 1

- Restore a critical system and time it
- MFA on every remote and admin login
- Patch internet-facing systems first

Week 2

- Look at yourself like an attacker
- Cut back admin rights, local accounts too
- Prove one backup copy is out of reach

Weeks 3–4

- Test how you reach everyone without email or phones
- Update the offline call list
- Check support contracts, spares and lead times

Day 30

- Score again: charlesaunger.com/cyber-score
- Tell the board in money and minutes
- Set the next 90 days

WHERE YOUR EFFORT GOES

Quick Wins

DO THESE NOW

- MFA everywhere
- Patch internet-facing
- Offline backup check
- Offline call list
- Name floor walkers

Big Moves

PLAN AND FUND NOW

- A real DR run
- Recovery order rehearsed
- Replace end-of-life kit
- Full device inventory

Keep Ticking

SCHEDULE THEM

- Policy review
- UPS and cooling tests
- Audit findings closed

Paper Only

STOP COUNTING THESE

- Tabletop-only exercises
- Policies nobody enforces
- Certificates as proof

Less effort → More effort



BEFORE THE BOARD ASKS

Are You Really Doing the *Basics?*

The basics are still where attackers get in. Do not presume anything: for each one, be able to show the evidence and the date, not the policy.

01 Update and Patch, All the Time
The date critical patches last reached every system, and the exceptions list.

02 Monitor Everything
The last alert someone investigated and acted on, and when.

03 User Account Management
Leavers and dormant accounts removed, local accounts included, with a date.

04 Elevated Permission Management
Who holds admin rights, reviewed and reduced, with a date.

05 Back Up, and Test the Backups
The last real restore, how long it took, and an offline copy out of reach.

06 Disaster Recovery & Business Continuity
The last rehearsal with the people who would do it, and what broke.

07 Check the Connections
Every external link traced, owned or closed.

08 Do Not Presume Anything
Seen for yourself, not reported to you.

DAY ZERO IS NOT GOOD ENOUGH ANYMORE.

Attackers care about what applies to the environment they are breaking into. Know what is exposed before they do.

DO IT NOW

- Update and Patch
- Elevated Permission Management
- Back Up
- Do Not Presume Anything

THIS MONTH

- Monitor Everything
- User Account Management

THIS QUARTER

- Disaster Recovery & Business Continuity
- Check the Connections



RED ALERT

When It All Goes Wrong.

Stay calm, communicate and move the dial. This is what still works when the plan meets reality.

01 Isolate
Contain it before you fix it.

→

02 Focus
The right people on the right problems.

→

03 Communicate
Calm, regular, honest updates.

→

04 The Goal
Recovery, not the witch hunt.

→

05 Recover
What matters first, then build back stronger.

THE GRAB KIT: IF EVERYTHING IS GONE

- **Offline Call List** — Staff, vendors, insurer, regulators, police.
- **Out-of-Band Comms** — A tested way to reach everyone without email or phones.
- **Floor Walkers** — Named people to update staff when screens go dark.
- **Deputies With Authority** — Someone can decide if leaders are unreachable.
- **Downtime Forms** — Printed, current, and practised with.
- **Power You Trust** — Generator tested on load, fuel and UPS checked.

"Are We Secure?"
No guarantees. The board can have the truth: protected, exposed, tested.

Memories Are Short.
Lock in new habits during recovery, before the urgency fades.

Paper Doesn't Protect You.
Attackers test what you do, not what you wrote down.

FREE DIGITAL TOOL

Get Your Cyber Readiness Score.

Put in the dates you last actually did each basic and get a score out of 100, your risk band and the three things to fix first. Private: nothing leaves your browser.

charlesaunger.com/cyber-score

General guidance, not professional advice. © 2026 Charles Aunger.