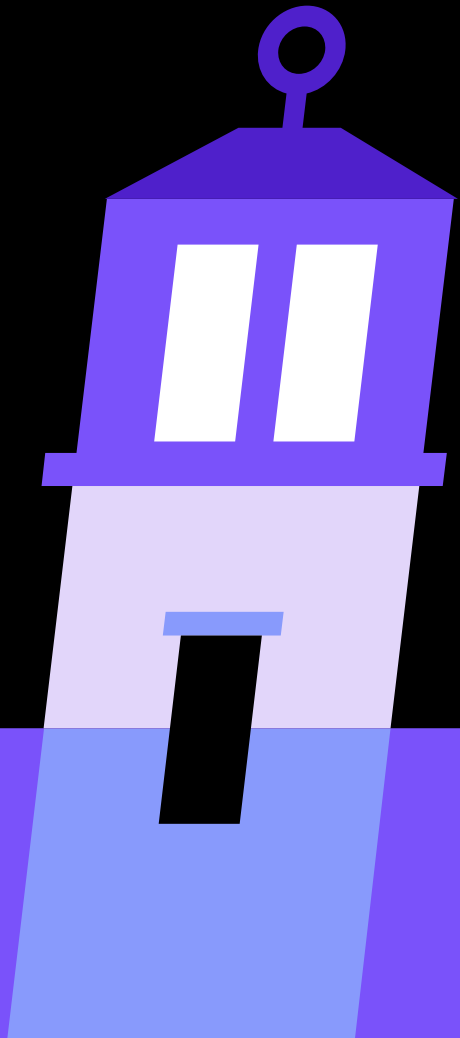
CHARLESTON

HYBRID
IDENTITY
PROTECTION

conf25



HYBRID IDENTITY PROTECTION conf25
CHARLESTON

Benjamin Cauwel

VP, Capgemini

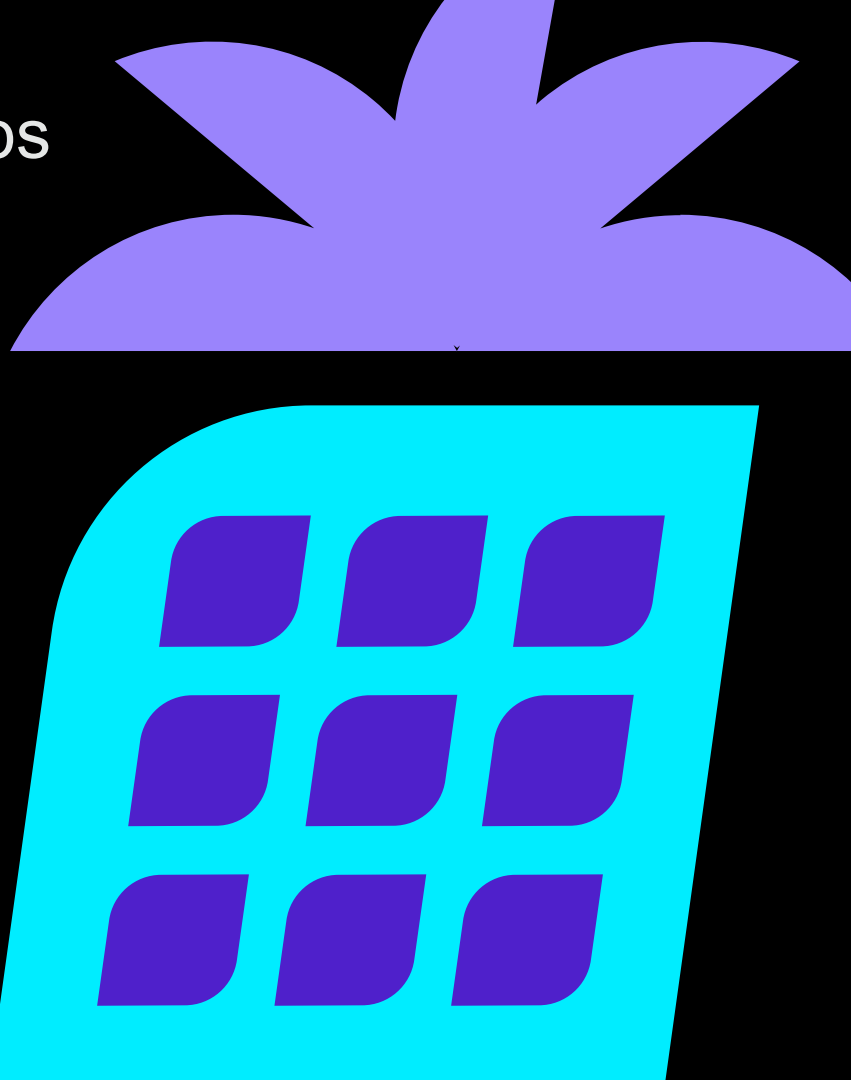
- 2004-2006: Systems Engineer
- 2006-2008: Consultant
- 2008-2010: Senior Consultant
- 2010-2020: Consultant / Senior Consultant / Manager
- 2020-2025: Manager / Senior Manager
- 2025-today: VP Head of Cybersecurity

Beyond Backups: Practical Steps to Build Operational Resilience

To quote Malcolm X, "The future belongs to those who prepare for it today."

This holds true in cybersecurity, where preparation is often the difference between business continuity and catastrophe.

Learn the must-have technical and functional steps to keep your operations humming and your organization afloat during a cyber crisis.



HYBRID IDENTITY PROTECTION conf25

CHARLESTON

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

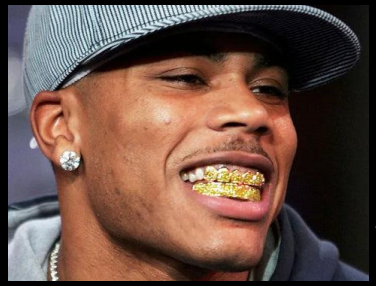
"All business, baby, it's all about the money"
Where's your money - ODB

Flashback from HIP 2024

- **Worldwide cybercrime costs are estimated to hit $10.5 trillion annually by 2025**, emphasizing the need for enhanced cybersecurity measures (Cybersecurity Ventures).
- **The average cost of a ransomware attack was $4.54M** (IBM).
- **The global average cost of a data breach in 2023 was $4.45 million**, a 15% increase over three years, highlighting the growing financial burden on organizations (IBM).
- **Ransomware is identified as the number one concern of the C-suite** in 62% of surveyed organizations, up 44% from 2022 (CFO).
- **Nearly half (47%) of companies now have a policy to pay ransoms associated with cybersecurity threats**, a 13% increase from the previous year (CFO).
- **Only 8% of businesses that pay ransom to hackers receive all of their data in return** (Sophos).
- Globally, **72.7% of all organizations fell prey to a ransomware attack in 2023** (Statista).
- **Extortion was involved in 27% of attacks**, indicating a growing trend in ransomware tactics (IBM Security X-Force 2023).
- **Backdoors were deployed in 21% of all incidents remediated in 2022**, while ransomware constituted 17% of the incidents (IBM Security X-Force 2023).

NIST CSF and where you put your $$$

- Can anyone please elaborate NIST CSF 1 for me?
  - Do you even follow this type of framework?
  - How mature is your company?
  - Where do you guys spend your $?



Nelly said:

“I put my money where my mouth is and bought a grill
20 carats, 30 stacks, let 'em know, I'm so fo' real”

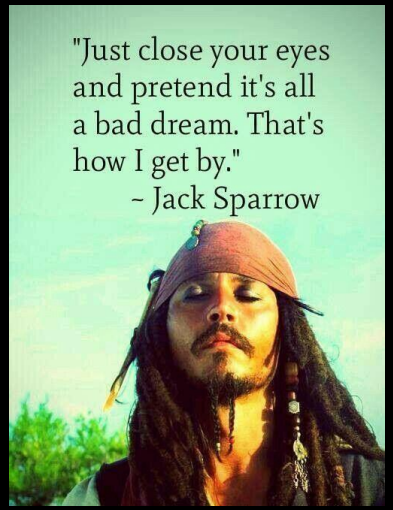
C-suite say:

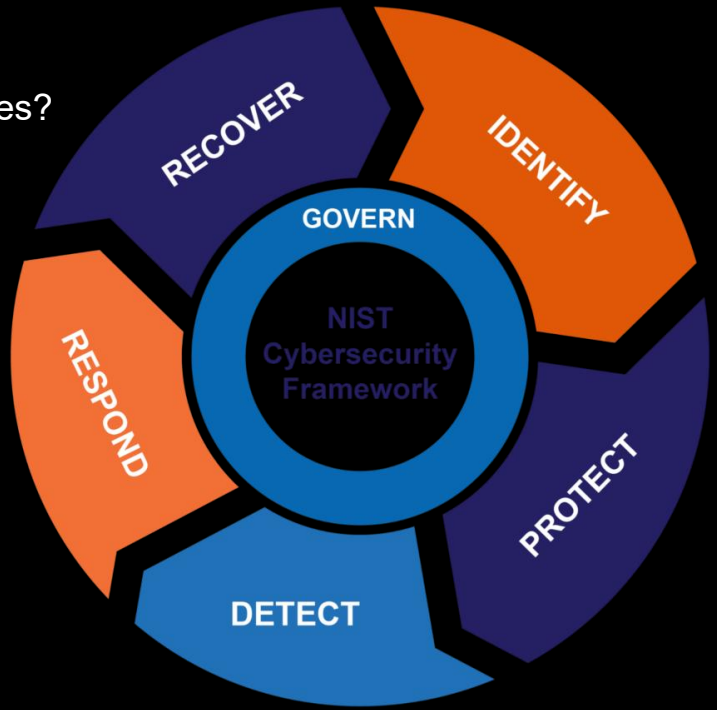
“Build a Bcase based on risk management & impact analysis ”

“tick boxes and invest on some pillars”

NIST CSF 2 main evolutions

- Can anyone please tell me the main difference with CSF 1?
  - Why have they added the governance brick?
  - Is your org actually working on the TOM?
  - Are you just adding some GRC interviews to tick the boxes?





HYBRID IDENTITY PROTECTION conf25 CHARLESTON

The ugly truth for most F500 companies

- Does anyone even have a clean CMDB?
- Self service Risk assessment with the watermelon effect
- Improvement? We are best in class

- Couple mill (3 years) for basic SIEAM/SOAR – no integration with other teams

- We have backups
- No end-to-end DRP exercise

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

- High level org context
- No risk management strategy
- What is supply chain?
- Basic RACI with no interop view
- Outdated procedures

- No tiering or EAM, little end-to-end IAM lifecycle
- Awareness campaigns
- Data classification myth
- Platform security

- No structure
- RCA is the key
- IR is externalized
- No plan = no mitigation

Buckle up, you're in for the ride of a lifetime

- Based on what we've just seen in the previous slide…

Travis Pastrana sums up what is about to happen in the next few months ;)

I hope you've enjoyed your lunch break, you get back to the office to this….

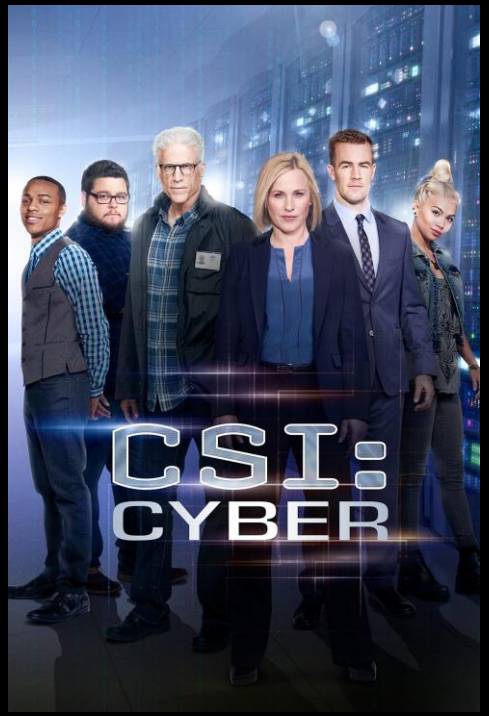
HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Overview of the next months

Phase 1: Exec fun

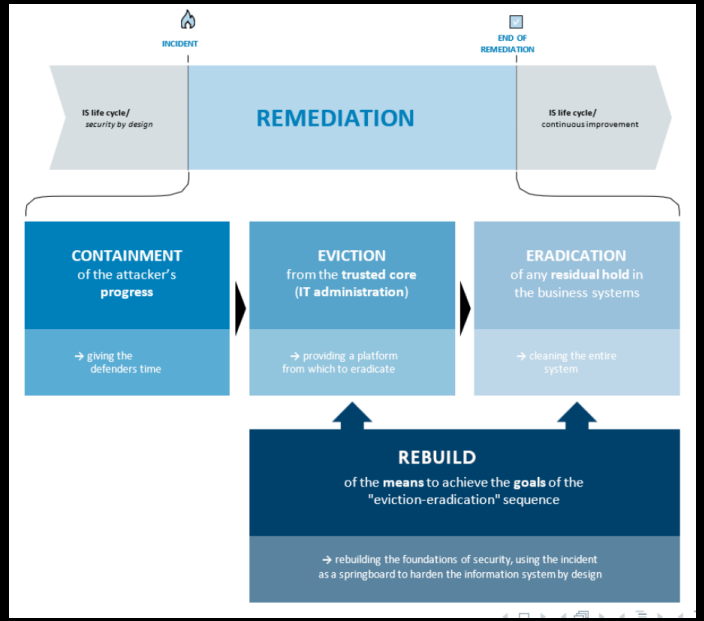
Phase 2: Lawyer up

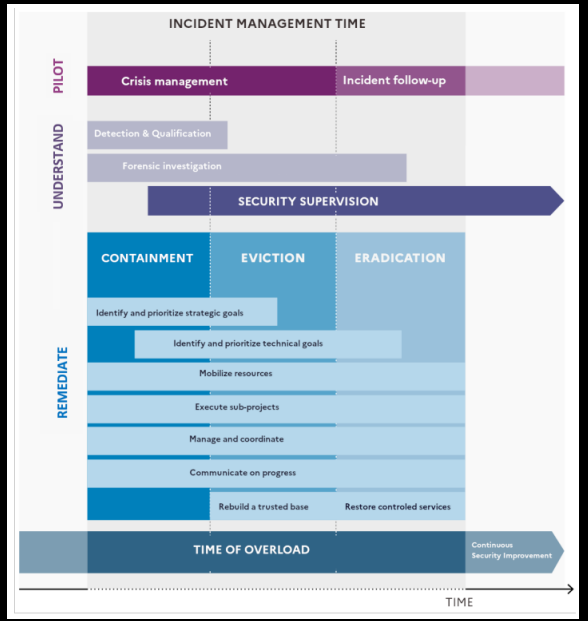
Phase 3: Drown



Quick focus on Phase 3 : CSI

Extract from ANSSI (the French National Cybersecurity Agency)





What happens in real life:

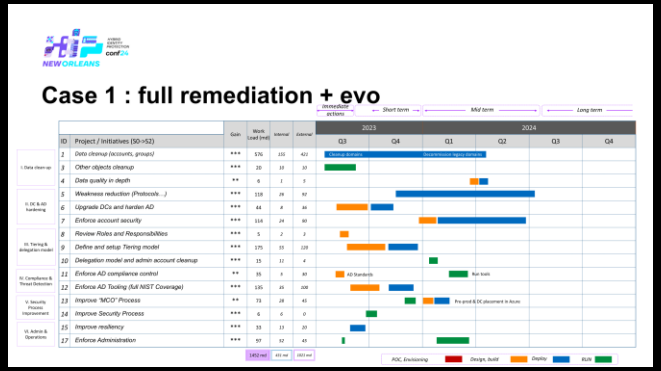
- Your untrained execs will be giving out orders
- Your understaffed teams will be mostly handling this exercise 24/7
- Your business will take weeks/months to get back online

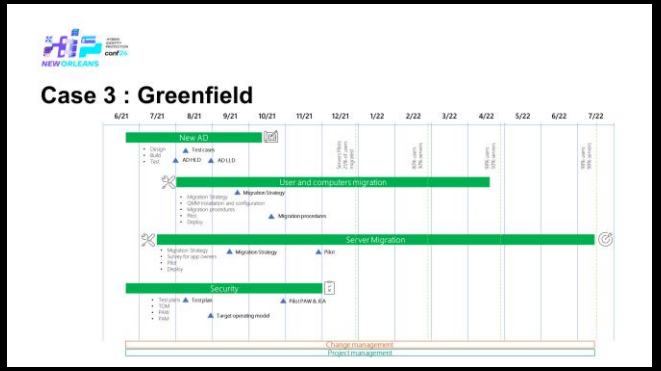
Time to come up with a plan

- Bcase : 12k users / 15k computers / 2.5k servers / hybrid identity
  - Purple Knight for AD score around 60%
  - Purple Knight for Entra score around 60%
  - Flat network
  - No governance

"I love it when a plan comes together"

Lieutenant Colonel – John "Hannibal" Smith





Whatever the scenario : 2M$ to 3M$ (without HW & licenses) and 1 year implementation with laser focus (realistic plan -> 2 to 3 years if no strong commitment)

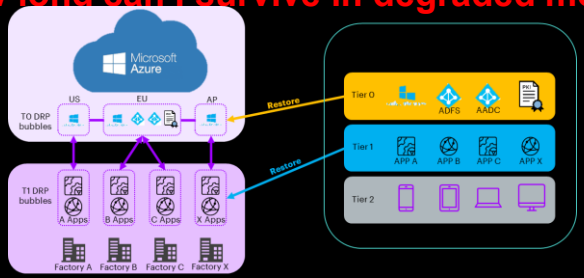
Real question… Can you wait for that long?

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

How about an MVP approach?

Understand your business… and it ain't IT

- What are the apps that make your business $$$?
- What IT infrastructure do they rely on ?
- Can I operate in closed silos ?
- How fast can I DRP/BCP ?
- How long can I survive in degraded mode ?



- Global MTTR is defined by how long you can survive in degraded mode
- Focus on MTTR for applications that make your business $$$
- Tabletop exercises 2 times per year
- Define all possible scenarios with decision trees

If you can steal an idea from someone's mind, why can't you plant one there instead?

What you need to remember

“The Matrix is a system, Neo…. But when you're inside, you look around, what do you see? Businessmen, teachers, lawyers, carpenters. The very minds of the people we are trying to save. But until we do, these people are still a part of that system…”

The key steps:

- If you’re IT, stick to IT (MVP approach)
- If you’re an exec, stick to decision making (planning & training are the key success factors)
- No one will criticize your actions if you can run the business during a cyber crisis / you will be frowned upon if you have no plan
- Once you have this approach down pat, you can plan for your 3-year evolution roadmap (not the other way around)

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

“If you don’t know me by now, I doubt you’ll ever know me”

KRS-One – MC’s act like they don’t know

linkedin.com/in/bencau
benjamin.cauwel@capgemini.com

Questions?


HYBRID
IDENTITY
PROTECTION
conf25
CHARLESTON