Several lessons, every CxO needs to know about

Yevhen Baliutov

Making world safer and more resilient since 2009

Worked across banking, telecom, pharma, tech, and critical infrastructure.

Father of 3

CISO, Raiffeisen Bank Ukraine

Academic director of Cybersecurity bachelor's program at KSE University (Kyiv)

Our agreement for the next 15 minutes

The main task for any leader is to simplify complex context

I’m not here to scare you

You're free to disagree

What did we have?

1 year

Strong belief, we are professionals

6000 employee

3 datacenters

Huge retail and digital business

~~Vaccination from COVID~~ Hybrid work setup

Key elements

Staff

Headoffice 2000

Retail 4000

Remote 30%

Contrators 300 +

Physical infrastructure

Offices 35+

Datacenters 3

Warehouses 10+

IT Infrastructure

Servers 4000+

User endpoints 8000+

Network

3rd party providers 200+

Retail infrastructure

Kiosks 150+

ATM 2000+

Branches 320+

Shops

Let's play the game. Guess. The most expensive incident since the full scale war started is ...

The BCM Challenges we faced

Real-World Complexity

Our BCM plans appeared comprehensive on paper, but crisis revealed critical gaps. The compounding nature of disruptions created scenarios we hadn't anticipated as simultaneous power outages, network failures, staff displacement, and cyberattacks required entirely new response frameworks.

Recovery time objectives became meaningless when infrastructure damage was ongoing. We had to shift from "recovery" mindset to "continuous adaptation" mindset.

For real crisis - you need plan for month, not days

Assumption Failures

Plans assumed single-point failures, not cascading system collapse across multiple dimensions simultaneously

Communication Breakdown

Primary and secondary channels failed together. You couldn’t reach anyone — not even by phone

Decision-Making Paralysis

Approval hierarchies too slow for rapidly evolving situations requiring immediate adaptation

Blocked 3rd party

Who will you trust in a real disaster?

People imagine you’re prepared. Reality is different.

Ask yourself 4 simple questions
Don't stop until you have answers different from:
"I don't know"

How will you operate if you physical infrastructure has been destroyed?

How will you operate if your IT network will be unavailable?

How will you operate if your critical staff will be unavailable?

How will you operate if your IT systems will be unavailable?

Optimism bias? Check the list

1 Check your vendors especially DC

Are they able to deliver services and BCM with your speed?

2 Wanna buy something?

Yes, you definitely need those 30 Starlinks and 30 generators. Any purchases during a crisis are more expensive and slower

3 Check network reservation

During tough moments - you need to be sure that your have 2nd provider operational

4 When did you perform failover?

Simulation or real one?

5 What about "process bottlenecks"?

Do you have backups? Did you test them in real situation?

6 100% workloads at the cloud?

What happens when your Direct Connect fails? Cook hybrid. Decrease risks

7 Can your people work remotely?

And what if your 1st VPN or VPN less agent is dead? Oh, you have just 1?

8 For sure, you've created several backups

Try aws nuke and check your readiness. Nope, nobody will dry to destroy your test environment. Go prod

9 What about fuel?

Dreaming about cloud workloads, don't forget to reserve enough fuel for weeks, not days

10 Do you have backup groups?

Your IT is the simplest to backup. What about call center? Back office functions?

11 Have contractors?

Forget about them during crisis. In such conditions - no obligations will be executed. Everybody will work on survival

12 Perfomance paradox

People tend to perform much better under stress. Even improvised solutions may outperform formal processes

No doubt, your cybersecurity teams are doing great job

Cybersecurity defense priorities during crisis

Perimeter Hardening

Enhanced DDoS mitigation, multi-layered firewalls, geo-blocking of high-risk regions, rate limiting on all external services including partners

Customer Protection

Enhanced fraud monitoring, customer security awareness campaigns, identity verification enhancements, 3FA for any money transactions

Team Coordination

Fusion center for security and operations, incident response playbooks automation, "first block - then think", law enforcement liaison

Identity & Access

Mandatory multi-factor authentication, privileged access management, continuous authentication monitoring, zero-trust architecture implementation

Threat Detection

Real-time security information and event management, behavioral analytics, threat intelligence integration, automated response protocols

Data Protection

Encrypted backups in multiple geographic locations, immutable backup strategies, rapid restoration capabilities, data integrity verification

Key Takeaways: preparing your organization for crisis

Start Preparation Now

Crisis preparation requires years of investment in redundant systems, trained personnel, and tested procedures. Once early indicators appear, it's already too late to start preparing

Challenge Assumptions

Traditional BCM and cybersecurity frameworks assume bounded disruptions. Geopolitical crisis like war, creates compounding failures across multiple dimensions simultaneously your plans must account for cascading complexity

Test Relentlessly

Paper plans fail under stress. Conduct regular simulations that test not just technical systems but decision-making processes, communication protocols, and human resilience under pressure

Invest in People

Technology and procedures matter, but organizational resilience ultimately depends on empowered, trained, supported people who can adapt rapidly to changing conditions and maintain operations despite extraordinary challenges

---

The experience of Ukrainian financial institutions demonstrates that survival during geopolitical crisis requires fundamental transformation of organizational culture, operational models, and security postures. Organizations that begin this transformation before crisis strikes gain decisive advantages in maintaining operations, protecting stakeholders, and emerging stronger when stability eventually returns.