From the Computer Room to the Board Room

By Robert "John" Bissell – Founder of the "*Operational Resilience Governance™ Initiative"*

In the fall of **1965**, I started my career in what was then called **Computer Operations**.

That probably dates me, but it also gives me a rather unique perspective on how much organizations and technology have changed over the past six decades.

There were no networks, no internet, no cloud, no cybersecurity departments, no smartphones, and no AI.

There was a computer room.

Inside were large machines, spinning tape drives, card readers, printers and stacks of punched cards.

Programs were assembled as card decks. Data was stored on cards or magnetic tape.

And much of what we would today call data security could be reduced to a few basic questions:

Is the computer room locked? are the backup tapes current and stored offsite? do we have backup run decks, and run books?

When a program was a deck of cards

There was something wonderfully tangible about computing in those days.

You could **see the program**, you could **see the data**, and you could **see the equipment**.

And you could understand, with reasonable clarity, what needed to be protected and who was responsible for protecting it.

Then the world changed.

The computer room became the world

Over the next six decades, I had the opportunity to watch—and participate in—an extraordinary transformation.

Computers became smaller and vastly more powerful, networks connected computers together, those networks connected organizations, the internet connected virtually everything.

Data moved from physical media to distributed systems.

Applications became dependent upon other applications, organizations moved infrastructure into data centers and then into the cloud, third parties became integral to the delivery of business services, mobile devices put computing power into virtually everyone's hands.

And now artificial intelligence is beginning to change how organizations operate and make decisions.

The computer room didn't disappear. It evolved—into the complex, interconnected environment that now supports virtually every aspect of organizational operations.

But something else changed along the way.

The amount of information required to understand and manage the organization grew exponentially.

Organizations matured

Over those same six decades, organizations didn't simply become more technologically sophisticated.

They became much more sophisticated in how they manage themselves, we've developed increasingly mature approaches to **financial oversight and governance**.

We've pursued Zero Defects, Quality Circles, Total Quality Control, Continuous Improvement, Just-in-time, IT Governance, Enterprise Risk Management, ISO, Six Sigma, Business Continuity, Disaster Recovery, Cybersecurity, Governance, Risk Management, and Continuity, and the list goes on.

We've developed disciplined approaches to project management through frameworks such as **PMBOK**.

Organizations today are vastly more capable of managing complex activities than they were when I walked into that computer room in 1965.

And that is a good thing.

But there is an interesting gap.

We as a profession have matured, but I would argue that our approach to communicating resilience to executives has not matured at the same pace.

The executive has a different problem

I don't believe executives and Boards have failed to take responsibility for resilience, quite the opposite.

The executives I have worked with understand that their organizations must be able to continue operating when things go wrong.

They understand that disruption can affect customers, employees, finances, reputation and the organization's ability to fulfill its mission.

They understand that resilience requires investment.

The problem is different.

There is simply too much information for an executive or Board to reasonably digest.

Consider what an organization can produce today:

Business continuity assessments.

Disaster recovery plans.

Cybersecurity assessments.

Enterprise risk registers.

Technology risk assessments.

Third-party assessments.

Business impact analyses.

Emergency management plans.

Exercise results.

Recovery testing.

Vulnerability assessments.

Dependency analyses.

Audit findings.

Corrective action plans.

The list can seem endless.

And the information may be valuable.

It may be accurate.

It may be necessary.

But expecting an executive or Board to personally assemble all of that information into a coherent understanding of organizational resilience is unrealistic.

That isn't an executive failure, it is a governance information problem.

Organizations and Executive management have already solved this problem.

Consider **financial condition**.

An organization generates an enormous amount of financial information every day.

Executives and Boards don't consume all of it.

They shouldn't.

The organization's financial disciplines collect, validate, consolidate and interpret that information and transform it into something executives can understand.

Revenue.

Assets.

Liabilities.

Cash flow.

Capital.

Financial performance.

Financial condition.

The Board doesn't need to become an accountant.

It needs to understand the condition of the enterprise well enough to govern it.

We've spent decades developing the disciplines necessary to make that possible.

Now consider resilience.

We have developed extraordinary capabilities.

Business continuity has matured.

Disaster recovery has matured.

Cybersecurity has matured.

Risk management has matured.

Emergency management has matured.

Technology management has matured.

The individual disciplines are doing important work.

But where is the equivalent executive view?

What is the organization's Resilience Condition?

That is the question I believe we haven't answered nearly as well.

From information to understanding

This distinction is important.

I don't believe the answer is to give executives **more resilience information**.

They already have plenty.

The answer is to transform the information being produced by the various resilience disciplines into a **coherent view of the organizational resilience condition**.

Executives need to be able to understand:

What must we be capable of delivering, how resilient are those critical business services today, where are the significant gaps, what evidence supports our assessment, how confident are we in what we're reporting, and what risks are we accepting, and why?

Those are not questions that belong to one organizational silo.

They cross the organization, and ultimately, they are questions of **executive responsibility**.

The role of the silos

I don't believe the answer is to eliminate the silos.

Quite the opposite.

We need them.

We need the expertise of cybersecurity professionals.

We need technology professionals.

We need continuity professionals.

We need risk professionals.

We need emergency management professionals.

We need facilities, supply chain, data, application and operational expertise.

The silos provide the capabilities.

Their expertise is essential.

But the executive doesn't need to become an expert in each of those disciplines.

The executive needs to understand what all of those capabilities mean **when viewed through the lens of the business services the organization depends upon.**

That is the missing translation.

Why I began the Operational Resilience Governance™ Initiative™.

ORG isn't intended to replace business continuity, disaster recovery, cybersecurity, risk management, emergency management or any of the other disciplines that contribute to organizational resilience.

Nor is it intended to tell those professionals how to do their jobs.

Instead, ORG is intended to provide an **Executive Governance Discipline™** that brings the relevant information together around the organization's critical business services.

The objective is simple:

Give executive leadership and the Board a meaningful way to understand and govern the organization's Resilience Condition.

That means moving from individual capabilities and disconnected reports toward an enterprise view.

From information…

to understanding.

From activity…

to condition.

From silo reporting…

to executive governance.

From the computer room to the Board room

When I think back to that computer room in 1965, the contrast is remarkable.

Back then, resilience could sometimes be reduced to:

Lock the door.

Protect the tapes.

Keep the machine running.

Today, a critical business service may depend upon hundreds of interconnected technologies, people, facilities, suppliers, applications, data sources and shared services.

The complexity is extraordinary.

But I believe the executive question remains surprisingly simple:

What is the condition of our ability to deliver what matters?

We have spent decades developing better ways to understand and govern financial condition.

We've developed extraordinary disciplines for managing quality, projects, risk, security and operations.

I believe resilience deserves the same level of executive maturity.

Not because executives have failed.

Because we haven't yet given them the right way to see it.

That is the idea behind **Operational Resilience Governance™**.

My resilience journey began in a computer room in 1965. Where will your journey take you?

In the next issue:

Look for another article titled “Why Now?” on September 25, 2026.

For more information on the Operational Resilience Governance Initiative, vist our website: https://operationalresiliencegovernance.com