acceligence

The best gift a CEO could give a CISO: a board-approved MVC

Insight

August 25, 2026

Category: cybersecurity

Tags: ai, mvc, prioritization

When an enterprise struggles with cybersecurity, the diagnosis usually starts with resources. The security organization needs more budget, more people, better tools, or all three.

That diagnosis may be accurate, but it is often incomplete. Additional resources cannot fully compensate for an enterprise that has not decided which business capabilities matter most. Every application arrives with an owner. Every business unit believes its work is critical. Every process has a constituency prepared to defend it. The CISO is then left with an impossible mandate: protect everything against an expanding set of risks, recover everything immediately, and do it within the constraints of the existing budget.

A view of the “Minimum Viable Company,” or MVC, gives the CEO and board a way to replace that ambiguity with clear business priorities.

Define the business that must survive

An MVC identifies the smallest set of capabilities the enterprise must continue operating, or restore quickly, to remain viable. It begins with business processes or the value chain rather than applications, infrastructure, or organizational charts.

For a bank, the irreducible core may include accepting and safeguarding deposits, moving money, extending credit, and meeting essential regulatory obligations. For an automotive parts manufacturer, it may include sourcing materials, making product, shipping product, selling product, and collecting payment.

Other work still matters. It simply may not carry the same consequence if it is interrupted for a day, a week, or longer. That distinction is essential. Most enterprises have hundreds or thousands of applications, vendors, data sets, facilities, interfaces, and operating dependencies. Asking IT and cybersecurity to treat all of them as equally critical

spreads attention and investment so broadly that the most important capabilities may remain underprotected.

MVC forces leaders to identify the company's *irreducible core*: the processes through which it serves customers, generates revenue, fulfills its central obligations, and remains a going concern. Once those processes are clear, the organization can map the technology, data, people, facilities, suppliers, and third parties required to sustain them.

This creates a practical connection between business strategy and operational resilience. The company is no longer protecting a generic inventory. It is protecting the specific capabilities on which its continued viability depends.

The hardest decisions belong with the CEO and board

The primary obstacle to MVC is rarely technical; it's organizational.

Establishing priorities means assigning different levels of importance, protection, and recovery to different parts of the business. Leaders are generally comfortable identifying their own functions as critical. They are less enthusiastic when another function receives a higher recovery tier or a larger share of resilience investment.

A list with 200 number-one priorities is simply an inventory. The CEO must therefore own the process, and the board should approve the resulting priorities and risk tradeoffs. The COO, CFO, CIO, CISO, General Counsel, business leaders, and other relevant executives should contribute their expertise. Public companies may also need input from investor relations and leaders responsible for regulatory disclosure and stakeholder communication.

The board does not need to debate individual firewall rules or application configurations. It does need to understand which capabilities the company intends to preserve during a severe disruption, how quickly they must be restored, what risks leadership is accepting elsewhere, and whether the investment plan reflects those choices.

This level of sponsorship prevents the CISO from being forced to make enterprise-wide business decisions through technical budget allocations. The business establishes the priorities. Cybersecurity and technology turn those priorities into controls, architecture, testing, and recovery capabilities.

Turn business priorities into a defensible technology footprint

Once the MVC is defined, it becomes actionable for the CISO.

Each core business process can be traced to the systems, identities, infrastructure, data, third parties, and operational resources that support it. That mapping allows the security organization to direct stronger controls and deeper resilience measures toward the areas where failure would create the greatest enterprise impact.

A critical payment platform may warrant stronger identity protections, more intensive monitoring, greater redundancy, tighter vendor requirements, more frequent recovery testing, and faster response commitments than a low-impact administrative system. Both require responsible security, with investment calibrated to consequence and recovery requirements.

This is strategic prioritization in practical form.

Lower-priority capabilities still receive baseline controls and risk management. They may accept longer recovery windows, lower levels of redundancy, or less intensive monitoring. Those choices become explicit, documented, and approved rather than hidden inside technical backlogs and budget constraints.

Without a board- and executive-supported MVC, the CISO often receives a mandate to protect everything equally with resources that make equal protection impossible. The result is diffuse investment, unclear accountability, and a security program forced to make tradeoffs that the business has never formally acknowledged.

With an MVC, the CISO has permission to concentrate people, money, and technology on what leadership has declared essential. The organization also gains an agreed recovery order for the day prevention fails.

That last point matters. A mature security strategy cannot assume every attack will be stopped. MVC connects prevention with business continuity, disaster recovery, crisis management, technology recovery, and third-party resilience. It answers a more useful question: what must still work, or return first, on the company’s worst day?

Use MVC to make better AI decisions

The MVC framework also gives executives a stronger way to evaluate AI and workforce decisions.

Many companies begin with a technical or financial question: which tasks can AI perform, and what cost can be removed? MVC adds the question that should come first: how close is this activity to the irreducible core, and what level of reliability does that position require?

The closer a process sits to the core, the higher the standards should be for accuracy, resilience, oversight, testing, fallback procedures, and accountable human judgment.

Direct customer engagement is an obvious example. Sales, service, and support often sit close to the mechanisms through which revenue, trust, reputation, and market share are created. AI can create substantial value in those functions. It can summarize customer history, recommend next actions, resolve routine requests, route issues more intelligently, and give employees faster access to relevant information.

Those opportunities should be pursued. The role assigned to AI should reflect the consequences of error.

A routine inquiry may be appropriate for automated resolution. A complex complaint, a sensitive account decision, or a high-value sales interaction may require human ownership and clear escalation. An organization can adopt AI aggressively while maintaining stronger safeguards wherever a poor outcome could damage a core customer relationship or interrupt an essential process.

MVC therefore helps leaders place automation where it improves the operating model and frees human attention for judgment-rich work. It also raises the reliability bar when AI is deployed inside the core. Cost efficiency becomes the result of deliberate design rather than the organizing principle for the decision.

A practical way to build an MVC

APQC's Process Classification Framework gives organizations a practical starting point by organizing common business processes into a consistent structure across industries. The framework supplies the map. Leadership supplies the judgment.

A practical MVC exercise begins by identifying the processes most directly tied to revenue, customer commitments, safety, liquidity, regulatory obligations, and the continued operation of the enterprise. Leaders then define the maximum tolerable disruption for each process and establish a realistic recovery order.

The next step is dependency mapping. Each priority process should be connected to the applications, infrastructure, data, identities, employees, facilities, vendors, and specialized knowledge it requires. This is often where the most important findings emerge. A resilient application may still depend on a single vendor, a fragile integration, an unavailable facility, or a small number of people with knowledge that has never been documented.

Leadership should then test the proposed MVC against severe but credible scenarios. A destructive cyberattack, cloud outage, telecommunications failure, critical supplier disruption, or loss of a primary facility can reveal whether the selected core is truly viable and whether its dependencies can meet the expected recovery objectives.

Once approved, the MVC should guide cybersecurity strategy, business continuity, technology architecture, third-party risk, crisis playbooks, capital allocation, insurance decisions, and AI deployment. It should also be revisited as the company's products, markets, operating model, and risk profile change.

Simplicity can be a sign of discipline

Berkshire Hathaway's famously sparse corporate website offers a useful illustration of the MVC mindset. One of the world's largest conglomerates maintains a site that is mostly text, links, shareholder information, and the materials stakeholders need.

Its design is text-based, fast, direct, and highly functional. It is arguably the purest MVC artifact on the internet.

The lesson is discipline: complexity should earn its keep.

Enterprises naturally accumulate systems, reports, products, controls, vendors, committees, and processes. Some remain essential. Others continue because nobody has required the organization to reconnect them to its purpose. Over time, the effort required to maintain the periphery can compete with the work that creates value at the core.

MVC gives leaders a structured way to make that distinction.

The gift is clarity

The greatest value of a Minimum Viable Company strategy is clarity.

It gives the board a concrete view of what must survive. It gives the CEO a framework for making difficult tradeoffs. It gives the CIO and COO a business-backed sequence for resilience and recovery. It gives the CFO a stronger basis for allocating scarce investment.

For the CISO, it provides something equally valuable: an explicit mandate to prioritize.

The CEO and board determine the MVC, while the CISO is well positioned to facilitate the process. Security leaders understand how business capabilities connect to technology, third parties, identities, data, and operational dependencies. By leading that discussion, the CISO demonstrates an enterprise perspective and helps senior management connect cyber risk to the way the company creates and protects value.

No organization can eliminate every risk or make every process equally resilient. Leadership can decide where reliability matters most, where recovery must be fastest, and where additional risk can be accepted.

The best gift a CEO can give a CISO is a clear, executive-backed, board-approved answer to one question:

What must this company be able to do on its worst day?