StoneSight
ADVISORY SERVICES

THE CYBERSECURITY CONFIDENCE GAP



Does your protection justify your confidence?

Confidence is easy to acquire. Protection must be demonstrated.

A room full of security screens can look reassuring. Their presence alone tells leadership little about whether someone will recognize a consequential threat and act in time. Enterprise security presents the same challenge: confidence must rest on evidence that protection works, not simply on the visibility of the investment.

A business can employ a chief information security officer, invest millions in cybersecurity, and undergo regular assessments while remaining exposed to an incident that stops its operations. Those investments matter, but their existence does not establish their effectiveness. Leadership must first determine what the business considers important to protect, what consequences it can tolerate, and whether its understanding of risk reflects reality. Without that foundation, an organization can spend too much protecting relatively inconsequential assets while leaving the systems, information, and relationships essential to its survival inadequately defended.

Spending ten dollars to protect a ten-cent item may make little economic sense. But that judgment changes if the item enables a production line, provides access to valuable information, or supports an obligation to a customer. Replacement cost alone does not establish business value. The consequences of losing an asset, the dependencies it supports, and the time required to recover all matter. Effective cybersecurity begins with understanding those relationships and making deliberate decisions about which risks to reduce, transfer, avoid, or accept.

Risk appetite expresses how much risk an organization is willing to accept in pursuing its objectives. That willingness must be considered alongside its capacity to absorb loss and the obligations it owes others. Management may be comfortable with disruption that its customers cannot tolerate, or accept exposure whose financial consequences it has underestimated. A stated appetite can therefore be dangerously miscalibrated. Establishing whether leadership's tolerance is informed, affordable, and appropriate is a central activity of effective risk management.

The business changes. Its assumptions must change too.

Consider a small town where residents routinely leave their doors unlocked. The person delivering food may be a neighbor's child whom the homeowner has known for years. Allowing that person inside reflects an assessment of familiarity, exposure, and trust. The homeowner is accepting risk, perhaps reasonably within those circumstances. But moving to a dense city center changes the context. Carrying the same assumptions into an unfamiliar environment could expose the household to consequences it never intended to accept.

The reverse move also warrants reconsideration. Someone relocating from the city to a quieter community may reasonably reassess the cost and inconvenience of existing precautions. Neither setting guarantees safety or danger; the point is that appropriate protection depends on circumstances. Familiarity also has limits: knowing the delivery person does not establish the trustworthiness of every substitute. Risk appetite should remain a considered judgment, supported by current information, rather than a habit carried forward from a different environment.

Businesses undergo comparable changes through acquisitions, expansion, outsourcing, new customer relationships, and technology adoption. A company that once held only its own information may begin holding customer data - or its customers' customers' data. That creates different dependencies, obligations, and potential consequences. Another company may discover that its proprietary information is the business's principal source of value. Restoring a stolen dataset from backup does not restore its confidentiality, exclusivity, or competitive advantage. An appetite formed before those changes may no longer fit the enterprise.

Operational dependence requires equally concrete examination. How long can the business function without its enterprise resource planning system? Can it receive orders, schedule production, ship goods, collect payment, and meet payroll? If financial systems become unavailable or their records cannot be trusted, can management close the books and report accurately to investors and the market? These questions translate cybersecurity into business tolerance. 'We can recover' offers little assurance unless leadership understands what can be recovered, how reliably, and within what period.



THE CONFIDENCE GAP

Confidence is a belief. Protection requires evidence.

More spending. The same exposure?

An incident alone does not prove that a security program was poorly managed. Equally, an uneventful history does not establish that the program works. Outcomes reflect exposure, adversary behavior, defenses, and chance. A company may operate with serious weaknesses because they have not been exploited, or because an intrusion has not been detected. Just as an unlocked suburban door can remain undisturbed for years, a vulnerable business can appear secure until circumstances change. Past experience must be interpreted alongside evidence about present exposure.

Excessive protection in the wrong place creates another confidence gap. Imagine an owner who installs a front-door lock, two deadbolts, a chain, and a door brace. Meanwhile, side windows remain open, rear windows are missing, and a weak back door gives an intruder a less visible place to work. Another front-door lock may provide less value than addressing those routes. The owner's spending follows the threat that commands attention, while the building's actual exposure remains poorly understood.

Cybersecurity programs can develop the same imbalance. Another platform receives funding while obsolete systems remain connected, departed employees retain access, and recovery arrangements remain untested. Layers of defense can be valuable, but their contribution depends on the risks they address and the capabilities needed to operate them. The relevant question is whether the next investment reduces a consequential exposure more effectively than the alternatives. A larger budget cannot answer that question by itself.

One company we surveyed, which will remain anonymous, hired a CISO after a breach stemming from obsolete servers. The incoming executive identified the risk, but the company never funded replacement of the obsolete infrastructure. Within 18 months, the CISO left because he believed he was ineffective in closing risks. The account does not establish whether alternative safeguards were implemented or another incident followed. It does illustrate why appointing a security leader cannot substitute for management decisions about funding, remediation, and accepted exposure.

Make confidence credible.

At StoneSight, we begin with leadership's determination of what matters and the risk appetite behind that determination. We examine whether that appetite fits the business's actual exposure, its ability to absorb loss, and its responsibilities to customers, investors, and others. We challenge assumptions about information value, operational dependencies, recovery, and the consequences of failure. Risk appetite calibration is a key activity because an inaccurate starting point can distort every subsequent decision about controls, expenditure, and assurance.

With that foundation, we examine the enterprise equivalent of accessible doors and ground-level windows: exposed services, obsolete systems, weak access controls, unmanaged assets, and third-party connections. Priorities follow business consequence and plausible routes to harm. Some entrances warrant stronger reinforcement because an attacker could work there longer without attracting attention. Others may justify a less costly safeguard. We seek protection proportionate to the exposure, supported by evidence rather than familiarity, fear, or the appeal of another technology purchase.

Our examination continues inside. A trusted delivery person may reasonably receive limited access, but that judgment should be deliberate and remain valid when the person, purpose, or circumstances change. In the enterprise, suppliers and contractors need access appropriate to their work, with clear ownership and oversight. An unfamiliar request requires verification. Shared entry codes that remain unchanged through years of departures and supplier changes undermine confidence about who can enter. We examine whether identities, credentials, privileges, and access decisions remain justified over time.

We explain the findings in English. Executives should understand which operation could stop, whose information could be exposed, how long recovery might take, and what decision is required. StoneSight's independent, CISO-led approach distinguishes documented intentions from demonstrated performance and makes assumptions, uncertainty, and assessment boundaries visible. We collaborate with existing security teams, including when the evidence supports concerns they have raised without adequate organizational support. Recommendations connect exposure to accountable owners, practical actions, and investment choices.

The objective is a defensible relationship between the risks leadership intends to accept and those the business actually carries. Sometimes that requires more funding; sometimes it requires redirecting expenditure, removing unnecessary access, or reconsidering an appetite that no longer fits. Confidence becomes credible when leadership understands what matters, recognizes how circumstances have changed, and can demonstrate that its decisions support the protection the business requires. That is the foundation StoneSight helps establish: informed tolerance, proportionate investment, and evidence that the organization can operate within the risks it has chosen to accept.



STONESIGHT
ADVISORY SERVICES

Move forward with informed confidence.

Understand your exposure.
Invest where protection matters.

---

advisory@stonesightadvisory.com

stonesightadvisory.com

© 2026 StoneSight Advisory Services, LLC.