Physical Security Risk Assessment for Mission Assurance and Business Continuity

The Leonidas Mission Assurance Framework™

Translating Risk into Operational Assurance and Enterprise Value

1. Executive Summary

Most organizations believe they are secure. Only a few can prove it.

This gap (between what we assume and what we can validate) is where risk becomes real loss. A security system that looks impressive on a proposal but fails during a crisis doesn't just cost money; it costs trust, continuity, and potentially the future of the business.

This paper presents a method for moving beyond that gap. We will show you how to assess your physical security posture, quantify risk in business terms, and align security with business continuity and resilience. The goal is simple:

to transform security from a perceived cost center into a verifiable risk management function that protects enterprise value.

Remember, the issue isn't a lack of security controls. The real problem is a lack of validated understanding. If this gap exists within your organization, a structured risk evaluation is critical. We see programs expand year after year, but the organization's ability to withstand a disruption doesn't seem to grow with them. Why?

Because the controls are not integrated, the risks are not quantified, and the execution is not tested.

Unquantified risk is unmanaged risk, and assessment is the foundation of assurance. Without it, you are not making informed decisions; you are making *expensive guesses*.

If your organization is making decisions without validated risk visibility, a structured assessment is critical.

Schedule an Executive Risk Briefing to identify where your exposure lies.

2. The Problem: Why Security Programs Fail

Organizations invest heavily in security. They install cameras, hire guards, and build fences. Yet, they remain exposed to threats that can cripple their operations. The reason is rarely a lack of hardware. It is a failure of process and perspective.

We see three common failure points here repeatedly.

1. Organizations frame security in purely technical terms.

A conversation about a new camera system becomes a discussion about megapixels and storage, not about the specific threat it is meant to deter or the business interruption it is meant to prevent. When security leadership cannot translate technical controls into financial impact, they lose the executive support needed to build a resilient program.

2. There is a lack of a validated, structured physical security assessment.

Decisions are made based on sales pitches, vendor recommendations, or what the company down the street did. This leads to disconnected lifecycle execution where systems are installed, turned on, and then forgotten.

3. Procurement often drives the process.

A security director is told to "*secure the facility*" with a specific budget, so they buy the most equipment they can afford. This cost-driven approach ignores performance. The result is a collection of systems that function in silos, with limited testing and no long-term sustainment plan.

The real risk here is quite insidious if you look at it closely. It creates a **false sense of security**. A leader looks at the wall-mounted cameras and assumes protection is in place. But an unvalidated system is a liability. It will only fail when it matters most, leaving leadership blindsided and with no defensible position.

3. The Executive Lens of Defensible Decision-Making

Security decisions are not technical decisions, but executive ones. Therefore, they require a framework that allows leaders to act with confidence, along with hope.

For a security investment to be sound, it must meet four criteria.

1. It must be *measurable*, meaning you can quantify the risk reduction.
2. It must be *justifiable*, tied directly to a financial impact, like avoided loss or reduced insurance premiums.
3. It must be *business-relevant*, connecting directly to your continuity and resilience goals. And finally;
4. It must be *defensible*. If an incident occurs, can you go to your board, your shareholders, or the public and clearly explain why your security decisions were appropriate?

This last point is the most critical here. If a security decision cannot be defended, it cannot be sustained. When a breach happens, the first question isn't "*Did the camera have enough megapixels?*" It's "*What was your process for identifying that risk, and why did you choose this control?*"

Our framework answers that question before it is asked. It begins with a structured physical security risk assessment. This assessment is the foundational document for your entire business continuity and mission assurance strategy. It turns subjective opinions about safety into objective data about risk.

4. Quantifying Risk With the Leonidas Model

To make security a business decision, you must translate it into the language of business: financial impact. We use two primary models to do this.

Total Cost of Loss

First, we calculate the Total Cost of Loss (K). This goes far beyond the cost of a stolen laptop or damaged equipment. The formula is:

$$K = C + CT + CR + CI - I$$

Here,

- **C** is the direct loss; the value of assets stolen or destroyed.
- **CT** is the cost of business interruption: the downtime, the lost productivity, the delayed shipments.
- **CR** is the cost of response and recovery; overtime, forensic investigations, legal fees, and system repairs.
- **CI** covers the indirect impacts: the reputational damage, the loss of a key contract, the regulatory fines, and
- **I** accounts for any insurance offsets.

The actual visible loss is often only a fraction of the total impact. A single security incident, for instance, can trigger a cascade of costs that far exceed the value of the physical assets involved. Consider the Colonial Pipeline ransomware attack in 2021. The direct ransom payment made headlines, but the real cost was the shutdown of a major fuel pipeline, leading to supply shortages, panic buying, and massive economic disruption across the Eastern United States[1].

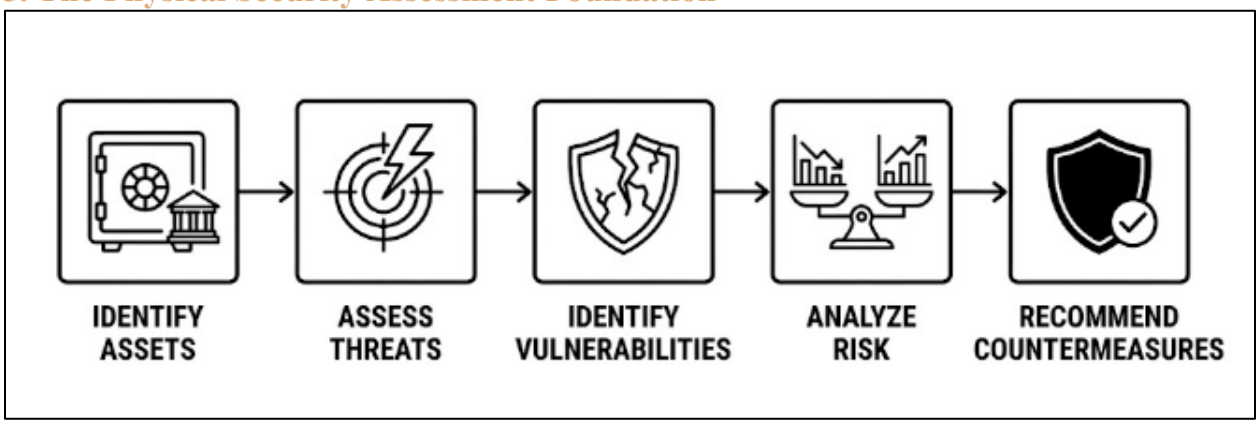
Annualized Loss Expectancy

Second, we use Annualized Loss Expectancy (ALE). This is a simple but powerful calculation:

$$ALE = Impact \times Probability$$

Estimating the potential financial impact of an event and the likelihood of that event occurring in a given year, we can prioritize investments. If a specific vulnerability has a high ALE, mitigating it becomes an urgent business priority rather than just a "security recommendation." This model helps leaders justify investment, allocate resources effectively, and make decisions that are both financially sound and defensible.

5. The Physical Security Assessment Foundation



[1] U.S. Government Accountability Office. (2022). *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Energy Sector*. GAO-22-105125.

Everything we have discussed (defensible decisions, quantified risk, operational resilience) starts with a single step: a *structured, validated physical security assessment*.

Without this assessment, you are flying blind. You cannot know if your risk is measured or merely assumed. You cannot know if your controls are verified or just present. You cannot know if your decisions are justified or simply expensive.

A business continuity plan, for example, written without a validated physical security assessment, is a dangerous document. It is built on assumptions, not evidence. It assumes your people can access the facility, your servers have power, and your communication lines are intact. If physical security fails, those assumptions are the first to crumble.

Our assessment methodology, on the other hand, adopts the Physical Security Professional (PSP) certification standards to follow a proven five-step process[2]:

1. **Identify Assets:** What are we protecting? (People, data, equipment, brand reputation)
2. **Assess Threats:** What are we protecting against? (Theft, vandalism, cyber-physical attacks, natural hazards)
3. **Identify Vulnerabilities:** Where are our weaknesses? (Gaps in fencing, single points of failure in power, poor access control)
4. **Analyze Risk:** What is the likelihood and impact of a threat exploiting a vulnerability?
5. **Recommend Countermeasures:** What specific, value-engineered solutions will reduce that risk to an acceptable level?

This process forces us to ask three core questions:

What is at risk?

Where is the exposure?

How can it be exploited?

Remember, if it hasn't been assessed, *it hasn't been validated*.

6. Understanding Risk: Threat, Hazard, Vulnerability

Before we can manage risk, we must understand its components. Three distinct elements combine to create a risk scenario.

The Threat

A threat is anything with the potential to cause harm. This is the actor or force. It could be an adversarial threat, like a disgruntled employee or an organized criminal group. It could be a natural threat, like a hurricane or an earthquake. The Metcalf sniper attack in 2013 is a perfect example of an adversarial threat.

For example, in 2013, an unknown individual with a rifle targeted a critical power substation in California (Metcalf sniper attack), showing how a single actor with a weapon could threaten a massive piece of national infrastructure. The attack in 2013 caused losses of up to $15 million, but it was unable to cause widespread outages due to power rerouting.[3]

---

[2] ASIS International. (2019). *Physical Security Professional (PSP) Examination Content Outline*. ASIS International.

[3] Federal Energy Regulatory Commission. (2014). *Arizona Public Service Company – Metcalf Substation Report*. FERC.

The Hazard

A hazard is the source of the danger. For a substation, the hazard is the high-voltage equipment itself. For a chemical facility, it is the hazardous material. The hazard doesn't act on its own; it requires a threat to trigger it.

The Vulnerability

A vulnerability is a weakness that a threat can exploit to cause harm. For example, in the North Carolina substation attacks in 2022, the vulnerabilities included a lack of physical barriers, insufficient surveillance coverage, and reliance on a single point of failure in the power grid[4]. The attackers didn't need advanced technology; they simply needed to exploit the vulnerabilities that already existed.

This shows that risk exists only when a threat and a vulnerability intersect. A hurricane is not a risk to a facility in the desert. An angry mob poses no risk to a facility with a hardened perimeter and no public access. Effective assessment requires understanding the specific adversary.

We must know who they are, how they operate, and what they are targeting. You cannot manage a risk without understanding the adversary that might seek to exploit it.

6. Layered Security: The 4Ds and Defense-in-Depth

Security is not a single wall, but a series of layers. A truly resilient security program uses a defense-in-depth strategy built around the 4Ds: Deter, Detect, Delay, and Respond.

- **Deter** is the first line of defense. Signs, lighting, visible cameras, and a security presence all send a message: "This is not an easy target." The goal is to convince a potential adversary to pursue an easier opportunity.

[4] Federal Energy Regulatory Commission. (2023). *FERC Staff Report on the December 2022 Attacks on Duke Energy's Moore County, North Carolina Substations*. FERC.

- **Detect** is the ability to know an incident is occurring. This is where sensors, alarms, and video analytics come into play. Early detection gives you time.
- **Delay** slows the adversary down. Fences, bollards, locks, and access control systems all add time. Time is your most critical asset because it allows your response to arrive.
- **Defend** is the decisive action that stops the threat. This could be a guard force, law enforcement, or even a remote lockdown procedure.

No single control provides security.

A fence without detection is just an obstacle.

An alarm without response is just a noise.

Effectiveness is achieved when these layers work together as a cohesive system. As an adversary moves inward (from the perimeter, to the controlled boundary, to the interior zones, and finally to the critical asset), the security measures should intensify and integrate. Security strengthens when layers are properly designed.

8. Access Control as Risk Control

In modern organizations, access control is far more than an "administrative" task for the HR department. It is a primary mechanism of risk control.

We must have clear answers to four questions:

Who has access?

What access do they have?

When is that access permitted?

And how is that access monitored?

Answering any of these questions with "I'm not sure" creates a vulnerability.

Uncontrolled access is one of the most common (and most preventable) sources of risk. It can manifest in many ways. It might be a former employee whose badge is still active. It might be a contractor who has access to sensitive data rooms. It might be a door propped open for convenience, bypassing the entire electronic system.

For instance, 63% of IT decision-makers admit that high-sensitivity access within their organization is not properly secured. Similarly, over half (56.4%) of healthcare organizations reported a breach in which a third party accessed their network in the past year. Users often have more privileges than they need, with 20% typically having excess permissions.[5]

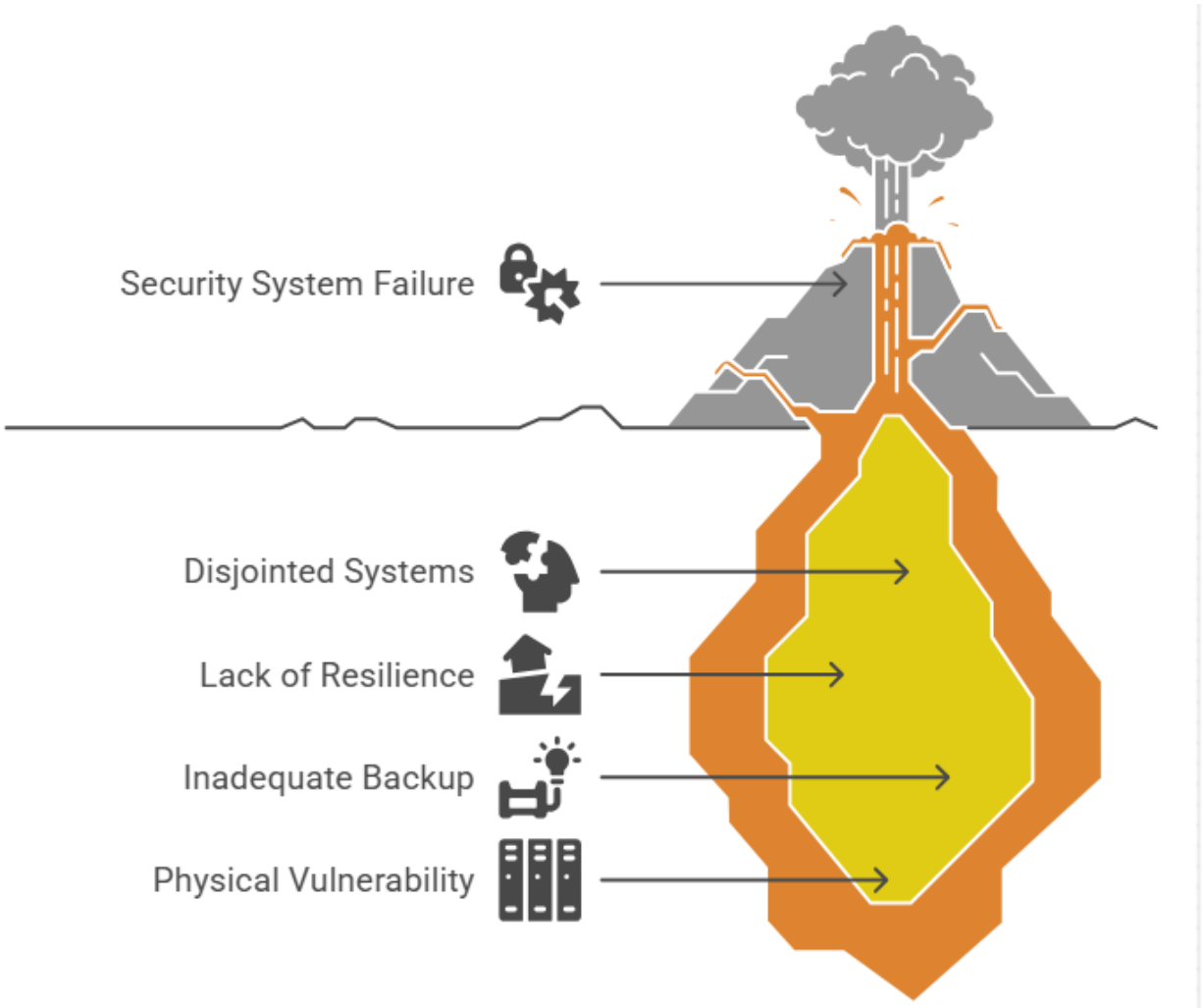
Effective access control also requires understanding the concept of "least privilege." A person should only have the access necessary to perform their job function. A marketing executive does NOT need 24/7 access to the data center. Similarly, a cleaning crew does not need access to the executive offices after hours. Strictly managing these permissions, we can reduce the risk of malicious acts while limiting the potential impact of human error.

[5] Gellert, G. A., Borgasano, D., Palermo, R., Gellert, G. L., & Kelly, S. P. (2025). Third-Party Access Cybersecurity Threats and Precautions: A Survey of Healthcare Delivery Organizations. *Applied clinical informatics*, *16*(5), 1518–1530. https://doi.org/10.1055/a-2713-5725

9. System Integration and Resilience

Security systems cannot operate as isolated silos. They must function as a unified, resilient ecosystem. This means your access control, video surveillance, intrusion detection, and fire and life safety systems must all communicate.

When systems are integrated, an event in one triggers a coordinated response in another. A forced door (intrusion detection) can cause a nearby camera to pan and zoom (video surveillance) and lock down adjacent access points (access control). This integration creates an efficient, automated reaction that human operators simply cannot match.



But integration is only half the equation. Resilience is the other half. We must ask critical questions. Do these systems function under stress? If we lose the main power, is there backup power? How long will it last? If a primary network line is cut, is there a redundant path for communication? Are critical components, like servers and controllers, physically protected from tampering or damage?

Disjointed systems create gaps. A system that fails under stress provides no assurance. The goal is to build an architecture that can withstand failures, whether from a cyberattack, a physical attack, or a simple power outage. True resilience is preventing a failure. It ensures the system continues to operate even in the event of a failure.

The 2021 Texas power crisis showed this principle on a massive scale. When the electrical grid failed, facilities with backup generators and redundant fuel supplies maintained operations. Those without backup power lost everything from security cameras to access control systems, leaving them blind and vulnerable at the worst possible moment[6].

10. Response Capability

We often say this: detection without a response capability is notification, not protection. It is one thing to know a door is being forced open. It is quite another to have the capability to do something about it.

An effective security program depends on three elements for its response capability.

First, you need **trained personnel**. Guards, supervisors, and even key employees must know their roles and have the authority to act. Training cannot be a one-time event. It requires regular drills, scenario practice, and performance evaluation.

Second, you need **defined protocols**. What is the exact procedure for a forced entry? For a fire alarm? For a suspicious person? A written plan that no one has practiced is not a plan. It is a liability.

Third, you need **reliable communication systems**. Radios, intercoms, and mass notification systems must enable instant, clear communication among the control room, field personnel, and first responders.

Response must be coordinated. The security team cannot act in isolation. Their actions must seamlessly integrate with local law enforcement, emergency medical services, and the organization's own emergency response team. A well-rehearsed, coordinated response can turn a potential crisis into a manageable incident.

Studies show that a two-minute delay in response can double the cost of a security incident[7]. Every second counts. Without a capable response, your detection systems only tell you how badly you have been hit.

11. The Human Element and Operational Discipline

We can design the most sophisticated security system in the world. But its ultimate effectiveness depends on people. Technology supports security. People execute it.

The human factor is the most variable and, often, the most critical. Effectiveness depends on consistent training, ongoing awareness, sound decision-making under pressure, and strict adherence to procedures. A guard who fails to challenge a person tailgating into a secure door has just bypassed a million-dollar access control system with a moment of inattention.

We use an Orders Framework to provide clarity and structure for security personnel.

General Orders

General Orders establish the overarching rules and code of conduct. They define the guard's fundamental responsibilities. For example, a General Order might state: "*I will remain alert and observe all activity within my assigned area.*"

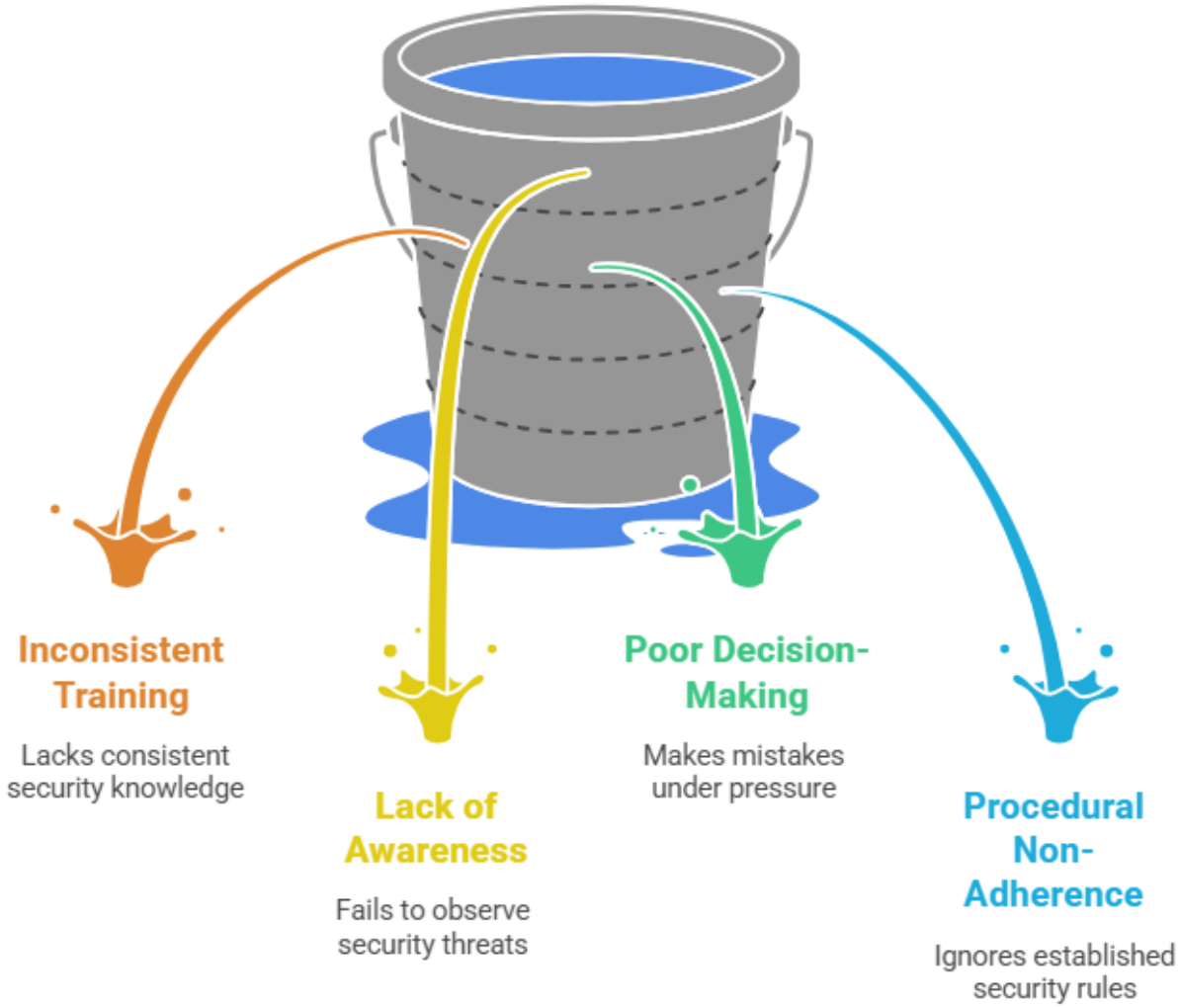
Post Orders

[6] Federal Energy Regulatory Commission. (2021). *The February 2021 Cold Weather Outages in Texas and the South Central United States*. FERC, NERC, and Regional Entity Staff Report.
[7] Security Executive Council. (2020). *Response Time and Incident Cost Analysis*. SEC Research Brief.

Post Orders are site-specific. They detail the exact procedures for a given location, such as how to conduct a patrol or operate a specific gate. A Post Order might say: "*Every hour, inspect the rear loading dock door for signs of tampering.*"

Special Orders

Special Orders are dynamic updates used for temporary situations, such as a facility shutdown or a specific threat alert. A Special Order might instruct: "*For the next 72 hours, require two forms of identification from all after-hours visitors.*"



When these three levels of orders are clear, consistent, and enforced, they create operational discipline. This discipline ensures that the human element becomes a reliable layer of security, rather than a potential vulnerability. It turns a group of individuals into a cohesive security force.

Research from the Security Executive Council indicates that over 70% of security breaches involve human error or procedural failures[8]. People are your greatest asset when properly trained. They become your weakest link when you ignore the human factor.

[8] Security Executive Council. (2021). *Human Factors in Security Breaches: Annual Report*. SEC.

12. Testing, Validation, and Continuous Improvement

A security system that is not tested is a system that is assumed. And assumptions fail under stress. A mature security program does not stop at installation. It moves into a cycle of continuous testing, validation, and improvement.

Testing methods should be varied and rigorous:

1. **Functional testing** verifies that individual components are working. Does that camera have a clear picture? Does that lock engage when the badge is presented? This is the baseline.
2. **Scenario-based exercises** put the system to the test. What happens if a fire alarm triggers while an unauthorized person tries to tailgate through a secured door? These exercise show how different systems and people interact under realistic conditions.
3. **Tabletop simulations** bring leaders together to walk through a scenario. They test communication, decision-making, and coordination without a physical event. These are low-cost but high-value.
4. **Red teaming** takes it a step further. A dedicated team attempts to physically breach security to identify real-world weaknesses. Red teaming often finds gaps that no audit or checklist ever finds.

Each test provides data. That data should flow into a continuous improvement loop. If a red team successfully breaches the perimeter, you fix that gap and you analyze why it happened, update your procedures, retrain personnel, and then test again.

This cycle builds assurance. It moves you from a reactive posture to a proactive one, where you strengthen your program based on evidence rather than just the passage of time.

The Department of Homeland Security recommends at least two full-scale exercises per year for critical infrastructure facilities[9]. Most organizations conduct none.

13. Physical Security and Business Continuity Are Interdependent

In many organizations, physical security and business continuity operate as separate functions. This is a dangerous separation. In reality, they are two sides of the same coin.

Business continuity (the ability to keep critical functions running during a disruption) depends entirely on the integrity of physical security. Your continuity plan might call for moving operations to a secondary site. But can your employees access that site? It might require using backup servers. But are those servers in a physically protected and access-controlled location? It might rely on communication systems. But are those systems vulnerable to physical sabotage?

If physical security fails, your business continuity plans do not execute under ideal conditions. They execute under degraded conditions. Or they fail entirely.

A perimeter breach might lead to a facility lockdown, preventing essential personnel from entering. A loss of access control could mean losing accountability for who is in the building, creating a massive safety risk during an emergency.

The chain of causality is clear. No assessment leads to no validation. No validation leads to no real protection. No real protection means your business continuity plan is a fiction.

[9] Department of Homeland Security. (2022). *Critical Infrastructure Resilience: Exercise and Testing Guidelines*. CISA.

Consider a manufacturing plant that experiences a forced entry overnight. The security team discovers the breach at 6 AM and locks down the facility for investigation. The day shift cannot enter until 10 AM. That four-hour delay costs the company $500,000 in lost production. The security failure directly caused a business continuity failure[10].

14. Executive Considerations in Assessment

A truly effective assessment requires a blend of hard data and human judgment. It is about understanding the organization's unique context and risk appetite.

Executives drive the assessment by answering three foundational questions.

What is at risk?

This is the asset inventory, but it includes intangible assets like intellectual property and reputation. A data center may contain customer information worth far more than the hardware itself.

Where is the exposure?

This is the vulnerability analysis that identifies the cracks in the system. Exposure might exist at a shipping dock, a visitor entrance, or a shared parking garage.

How can it be exploited?

This is the threat profiling that considers the capabilities and intent of potential adversaries. A disgruntled former employee poses a different threat than an opportunistic thief.

A key outcome of this process is **value engineering**. This is the practice of allocating resources based on risk rather than a vendor's suggested list. It means optimizing cost versus effectiveness. Instead of installing the most expensive camera system, you might find that a combination of physical barriers and well-trained guards delivers the best protection for your specific threat profile.

The assessment must also consider **organizational integration**. Security does not exist in a vacuum. The security team must be in line with operations, information technology, facilities, and safety. This integration ensures that security measures support business processes rather than hinder them.

[10] Ponemon Institute. (2021). *Cost of Physical Security Incidents Report*. Ponemon Research.

There is also the principle of **risk acceptance**. Not all risks can be eliminated. The goal is to reduce them to an acceptable level. However, any accepted risk must be documented, justified, and defensible. It must be a conscious choice made by leadership, not an oversight.

15. Security Maturity Model

To understand your organization's current posture, we use a maturity model. This model provides a roadmap for improvement, showing where you are and where you need to go.

Level	Description
Reactive	The organization responds after incidents occur. Security is seen as a cost of cleaning up messes.
Compliant	The organization meets the minimum standards set by regulations or insurance. Security is a checklist item.
Structured	The organization conducts formal assessments and has documented policies and procedures. Security is a defined function.
Integrated	Security is in line with operations, business continuity, and enterprise risk management. It is a valued business partner.
Assured	The organization operates a lifecycle-driven, continuously evaluated, and optimized security program. It is a source of competitive advantage.

Most organizations operate below the integrated level. This is where exposure remains highest. They may have systems and policies, but they are not in line with the business's true goals. The goal of any security program should be to reach the "Assured" level, where security is present, proven, and continuously improving.

A 2022 survey found that only 12% of organizations rated themselves as "Integrated" or "Assured" in their physical security maturity[11]. The remaining 88% operate with significant gaps.

16. Common Misconceptions

Several persistent misconceptions keep organizations from achieving a mature security posture. They are dangerous because they create a false sense of security that actually increases exposure.

"We have systems, so we are secure."

Having a system is not the same as having a validated, integrated, and tested program. A camera system that no one monitors is just a recording device. An alarm system with a 20-minute response time is just a notification device.

"Insurance mitigates risk."

Insurance is a financial tool for recovery, not a risk mitigation tool. It does not prevent the incident. It does not protect your reputation. It does not guarantee your business will survive the interruption. The North

[11] Security Magazine. (2022). *Security Maturity Benchmark Survey*. Security Media Group

Carolina substation attacks caused over $100 million in damages and massive operational disruption that no insurance policy could have prevented[12].

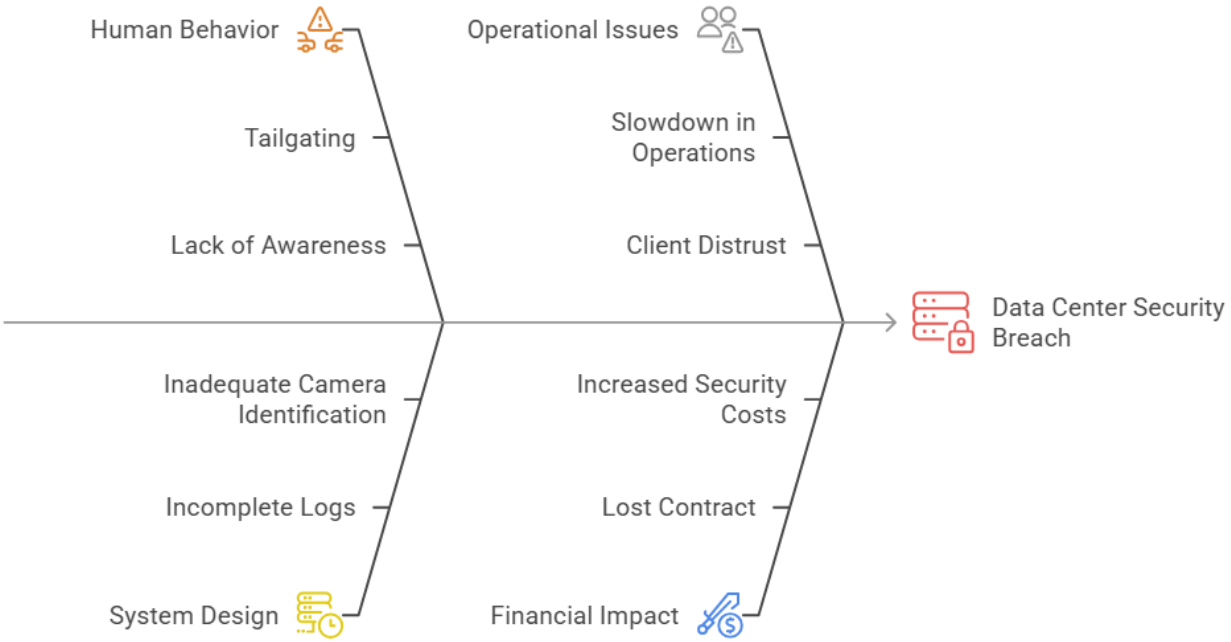
"Compliance equals protection."

Meeting a regulatory standard, like a specific fence height or a certain number of cameras, ensures you meet a baseline requirement. It does not ensure you are protected against a sophisticated threat. Compliance is a floor, not a ceiling.

"Security is a one-time investment."

Security is a lifecycle. It requires constant maintenance, updates, training, and testing. A system installed five years ago and never touched is no longer a security asset. It is a security risk waiting to happen.

17. A Failure Scenario



To bring this into focus, consider a common failure scenario.

An organization has a data center. It has a badge reader on the door and a camera in the hallway. A breach occurs. An unauthorized individual follows an employee through the door (tailgating) and gains access to a server rack.

After the incident, an investigation begins. The systems appear functional. The badge reader logs show the employee's access. The camera system recorded the hallway. But the logs are incomplete. There is no record of the tailgating event because the system does not track it. The camera footage shows the individual, but does not identify them.

Operations slow to a crawl as information technology and security scramble to contain the breach. Clients question the organization's reliability. A contract that was up for renewal goes to a competitor.

[12] Federal Energy Regulatory Commission. (2023). *FERC Staff Report on the December 2022 Attacks on Duke Energy's Moore County, North Carolina Substations*. FERC.

The incident ends, but the impact does not.

The organization spent money on security, but it failed because it was not designed to prevent or detect the most common vulnerability: human behavior. Security failures are rarely sudden. They are cumulative, the result of many small gaps and overlooked details that finally in line for an adversary to exploit.

18. What Effective Security Looks Like

So, what does the future state look like? What does it feel like to have an effective security program?

- It begins with **quantified risk**. You have a clear, data-driven understanding of your financial exposure.
- It includes **validated systems**. You have tested your controls and know they will function as designed under stress.
- It operates through an **integrated lifecycle**, where security is not a project but a continuous process of assessment, design, implementation, and improvement.
- It provides **executive-level reporting** that translates security performance into business impact.
- Ultimately, it is built on a foundation of **continuous evaluation**, always seeking to improve.

In this future state, leadership operates with clarity. There is no guessing. No fingers crossed. You know what is protected. You understand how it is protected. You can clearly articulate why every decision is defensible.

19. From Insight to Action

At this stage, the question is no longer whether risk exists. Risk is a permanent feature of the business environment. The question is whether that risk has been validated and understood.

You have a security program. You have systems in place. But are they working? Is your posture based on evidence or assumption?

Security systems that are not assessed are assumed. And assumptions fail under stress. The cost of doing nothing, or doing it wrong, is always higher. It is the cost of the incident, plus the cost of the systems that failed to stop it, plus the cost of the reputation you lose, plus the cost of the business you cannot conduct. That is the true price of a false sense of security.

20. Executive Call to Action

The first step toward defensible security and true business continuity is a structured assessment. We invite you to engage with the Leonidas Physical Security and Mission Assurance Assessment.

This engagement provides you with exactly what you need to move forward with confidence.

- You will receive a **physical security validation**, confirming whether your systems actually protect your assets.
- You will get a **threat and vulnerability analysis** that identifies your specific areas of exposure.
- We will provide **risk quantification** that translates those vulnerabilities into clear business terms.
- We will ensure **business continuity alignment**, connecting your security posture to your ability to operate.
- And you will receive **executive-level reporting** that gives you the clarity and confidence to make the right decisions.

If your current security posture cannot be validated, it cannot be defended. Do not wait for an incident to finds the gaps in your program.

Schedule a 30-minute Executive Risk Briefing. In the session, we will assess your physical security posture and determine how it impacts your business continuity and resilience.

It is a conversation that could save your organization from a future you cannot predict, but can prepare for!