The Reality of Risk

Understanding Perception Gaps in Access Control Security

Written by
David Vigor, End User Business Development Director

EBOOK

Contents

HID

Introduction: The Gap Between Actual and Perceived Risk

In a perfect world, organizations would assess security threats with pure rationality, implementing measures proportionate to the actual risks they face. But we don't live in that world.

Instead, perception often trumps data, and gut feelings override statistical probabilities. What feels secure frequently wins out over what actually is secure.

The gap between perceived and actual risk isn't just a curious psychological phenomenon — it's a serious vulnerability that puts organizations, their assets and their people at risk.

Understanding this gap is the first step toward closing it.

This eBook explores risk perception and its profound implications for access control. By examining why we misjudge threats, we can build better security strategies — ones that protect against real threats over perceived ones.

The Emotional Lens: How Feelings Shape Our View of Threats

Fear, anxiety, optimism and complacency don't just influence our security decisions — they can dominate them. Research from psychologists Daniel Kahneman and Amos Tversky has shown that humans consistently rely on emotional shortcuts, or "affect heuristics," when evaluating risk.

This explains why the vivid, emotional and immediate threats capture our attention and resources, while more statistically significant but less emotionally evocative ones often go unaddressed.

Consider the common scenario where organizations focus heavily on certain visible security aspects — like adding more cameras or implementing complex single-factor password policies — while neglecting statistically more vulnerable areas like employee security training or credential management systems. The visibility of cameras provides an emotional sense of protection, while the critical but less tangible work of developing modern security protocols and training programs lacks the same immediate emotional impact.

Similarly, organizations might prioritize addressing dramatic but rare threats while overlooking more common vulnerabilities that account for the majority of actual breaches.

The psychologist Paul Slovic has termed this the "risk as feelings" phenomenon. His **research demonstrates** that when emotions and analytical reasoning conflict in risk assessment, emotions typically prevail in decision-making.

Time Distortion: Why Tomorrow's Problems Feel Less Urgent Today

The human brain has a peculiar relationship with time — especially when it comes to evaluating risk. We systematically discount future threats, even when their potential impact far outweighs present concerns. Behavioral economists call this "hyperbolic discounting" — our tendency to choose smaller, immediate rewards over larger, future ones.

This cognitive bias makes long-term security planning particularly challenging. Investing in future-proofed security infrastructure often loses out to addressing immediate, more visible concerns — even when the former would provide significantly greater protection over time.

Climate change offers a powerful analogy. Despite overwhelming evidence of its catastrophic potential, the gradual, long-term nature of the threat makes it difficult for many to take immediate, costly action.

Similarly, the gradual obsolescence of security systems often fails to trigger urgent responses until after a breach occurs.

Security measures like encryption don't typically fail overnight. Instead, they grow gradually more vulnerable as computing power increases and new attack methods emerge. Organizations often delay upgrades — like the **33% of companies still using 125-KHz low-frequency proximity cards** — until a breach occurs (and the damage has been done).

The Group Effect: When Collective Thinking Clouds Judgment

Humans are social creatures, and our risk perceptions are profoundly influenced by group dynamics. Organizational psychologists have documented how “groupthink” can lead entire industries to collectively misjudge risks — with everyone heading confidently in the wrong direction together.

This social dimension of risk perception helps explain why entire sectors often share the same security blind spots, and why breaches tend to occur in patterns across organizations.

Consider the 2008 financial crisis. In the years prior, major financial institutions collectively ignored the risks of subprime mortgages. Individual risk managers who raised concerns were often dismissed because “everyone else is doing it.” The result was a systemic failure that affected the entire global economy.

In access control, we see similar patterns when organizations:

- Use outdated technologies with known vulnerabilities because they are still in wide use
- Blindly prefer on-premises access control system management over cloud-based systems
- Defer adoption of mobile access solutions due to institutional comfort with legacy card systems

Likelihood vs. Impact: The Critical Distinction in Risk Assessment

One of the most common flaws in risk perception is conflating likelihood with impact. A low-probability, high-impact event (like a coordinated attack on multiple access points) might receive less attention than a high-probability, low-impact event (like occasional tailgating at a building entry's turnstile).

Behavioral scientist Gerd Gigerenzer has found that people tend to struggle with statistical thinking, leading to systematic errors when evaluating rare but consequential risks.

Before 2020, many organizations underestimated the likelihood of a global pandemic disrupting their operations. The low perceived probability overshadowed the enormous potential impact. Those who had prepared for low-likelihood, high-impact events adapted more quickly.

When faced with statistics suggesting an event is extremely rare, many decision-makers essentially round down to zero — dismissing the risk entirely rather than evaluating its potential impact.

As the character in the film Dumb and Dumber famously said when told his chances were one in a million: "So you're telling me there's a chance."

We laugh at this, and yet it exemplifies a serious flaw in risk evaluation: the tendency to dismiss low-probability events rather than preparing for their potential consequences.

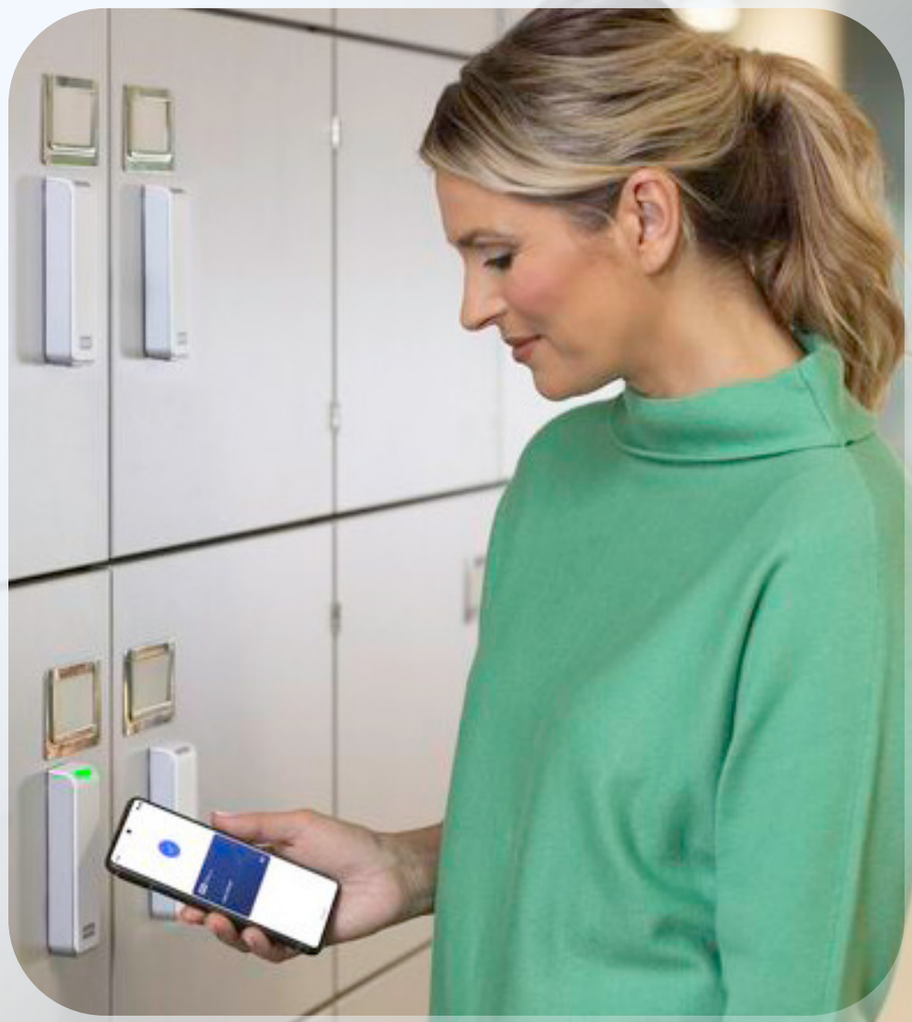
Value vs. Risk: The Balancing Act That Often Tips the Wrong Way

When potential value is high, risks often become invisible. This insight from behavioral economics explains why organizations frequently accept security compromises when pursuing valuable innovations or conveniences.

When cloud storage services first emerged, many businesses hesitated due to concerns about data security and loss of control compared to on-premises servers. However, the convenience, scalability and cost savings of cloud solutions quickly overshadowed these concerns, leading to widespread adoption — even before security standards and encryption practices were fully mature.

Economist Rory Sutherland has explored how perceived value can dramatically shift risk calculations. Organizations that initially resisted cloud adoption due to security concerns rapidly changed course once the business value became undeniable — demonstrating how high perceived value can make organizations more willing to accept (or overlook) security uncertainties.

The same pattern appears in physical access control, often in reverse. Organizations frequently resist adopting mobile access despite its enhanced security because of perceived implementation challenges. The familiar value of traditional systems and the immediate “cost” of change overshadow long-term security benefits, creating a risk calculation that favors the status quo — even when that status quo presents slightly more vulnerabilities.



From Theory to Reality: Learning from Historical Misjudgments

Historical examples of risk misjudgment provide valuable lessons that can improve our current security decisions. Looking at past failures reveals patterns in how organizations systematically underestimate certain types of risks.

The Titanic: “Unsinkable” Until It Wasn’t

The Titanic was famously deemed “unsinkable” based on theoretical models that failed to account for real-world variables and human behavior. This pattern repeats in security breaches, where theoretical security models often fail to account for how systems operate in practice.

Y2K: Did Preparation Prevent Disaster?

The Y2K bug presents a different lesson. While some view it as an overhyped risk because few major incidents occurred, this interpretation misses a crucial point: extensive preparation and investment prevented potential disasters.

This catch with successful risk mitigation is that it often becomes invisible, leading to the false conclusion that the risk was never real.

Security Lessons From History:

- Theoretical security models must be tested against real-world behaviors
- The absence of incidents doesn’t always indicate low risk — it may reflect successful mitigation
- Past patterns of security breaches often predict future vulnerabilities
- Human factors consistently undermine technical security measures

Conclusion: Greater Security Through Clearer Vision

The gap between perceived and actual risk isn't just an interesting psychological curiosity — it's a critical vulnerability that impacts organizations of all sizes across all industries. By understanding the cognitive biases that distort our risk perception, we can build security strategies that address real rather than merely perceived threats.

The future of access control security lies not just in advanced technologies, but in enhanced risk perception — seeing threats more clearly, evaluating them more objectively, and addressing them more effectively.

As security professionals, our greatest challenge isn't just implementing controls, but first ensuring we're solving the right problems. By bringing greater awareness to how we perceive risk, we can build truly effective security programs that protect what matters most.

HID's Access Control Security is Based on Decades of Experience, Not Assumptions

At HID, our approach to security isn't built on perception — it's built upon decades of real-world experience securing facilities across the world and in the most highly regulated industries. This expertise allows us to distinguish between perceived and actual risks, designing solutions that address genuine vulnerabilities, while always keeping in mind usability and convenience.

Want to learn more about our industry-leading access control solutions?
Visit **hidglobal.com/solutions/access-control-systems**

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 91 506 900
Asia Pacific: +852 3160 9800
Latin America: +52 55 9171-1108

For more global phone numbers click here

2026-06-15-pacs-reality-of-risk-eb-en

Part of ASSA ABLOY