Technology and Investment, 2026, 17(3), 200-215
https://www.scirp.org/journal/ti
ISSN Online: 2150-4067
ISSN Print: 2150-4059

Trust, Risk, and Investment Confidence in Defensive Cyber Deception Adoption

Daniel Ward

Department of Computer Science, Southern New Hampshire University, Manchester, United States
Email: d.ward@snhu.edu

How to cite this paper: Ward, D. (2026). Trust, Risk, and Investment Confidence in Defensive Cyber Deception Adoption. *Technology and Investment, 17,* 200-215.
https://doi.org/10.4236/ti.2026.173013

Received: July 3, 2026
Accepted: August 4, 2026
Published: August 7, 2026

Copyright © 2026 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

Defensive cyber deception technologies use decoys, honeytokens, simulated services, and false artifacts to create high-confidence signals when adversaries interact with resources that legitimate users should not touch. Although these tools are often discussed as technical controls, their adoption also depends on investment confidence: whether practitioners believe the capability is valuable, trustworthy, controllable, and worth organizational resources. This study examines that problem using secondary analysis of an existing deidentified survey dataset collected from industrial control system and operational technology professionals. The analysis tested whether investment confidence, self-efficacy/direct experience, social validation, and instructional support predicted adoption readiness and effective utilization beyond education, experience, and sector. The complete-case sample for the primary regression was 264. Demographics alone explained little variance in adoption readiness, R-squared = 0.026, $p = 0.225$. Adding perception-based predictors increased explained variance to R-squared = 0.639, $p < 0.001$. Investment confidence remained a significant predictor in the full model, beta = 0.251, $p < 0.001$, alongside self-efficacy/direct experience and instructional support. A second model showed that self-efficacy and social validation significantly predicted investment confidence itself. The findings suggest that defensive cyber deception investment is not only a tool-budget issue. It is a trust, capability, and risk-communication issue that must be addressed before organizations can treat deception as a credible security investment.

Keywords

Cyber Deception, Cybersecurity Investment, Investment Confidence, Operational Technology, Risk Perception, Technology Adoption, Trust

1. Introduction

Cybersecurity investment decisions are increasingly made in the face of uncer-

tainty. Leaders must decide which capabilities deserve funding, which capabilities add measurable value to existing controls, and which capabilities introduce unacceptable operational or governance risk. Defensive cyber deception presents this problem sharply. The technology can create high-confidence indicators when adversaries interact with decoys, honeytokens, simulated services, false credentials, or monitored artifacts. However, the same features that make deception useful can also make it difficult to fund and adopt. It is intentionally false; it must be trusted as a security signal and fit existing operational workflows.

This paper argues that the adoption of defensive cyber deception should be examined as an investment-confidence problem rather than solely as a security-engineering problem. Investment confidence is used here to mean the practitioner-level belief that a security capability is valuable, trustworthy, and controllable enough to justify organizational attention, resources, integration, and ongoing support. This is not equivalent to a formal return-on-investment calculation. Rather, it is a precursor to investment because organizations rarely fund and operationalize security capabilities that their professionals perceive as unclear, risky, untrustworthy, or difficult to manage.

The topic fits the scope of Technology and Investment because it concerns technology evaluation, technology risk, and investment under uncertainty. Defensive cyber deception is a technological capability whose investment case depends on perceived value, risk reduction, trust, and operational readiness. IBM's 2025 breach-cost reporting illustrates why faster identification, containment, role clarity, and incident-response preparation matter to business decision makers (IBM, 2025). The Gordon-Loeb model similarly treats information security spending as an investment problem in which expected loss, vulnerability, and marginal benefit shape the rational level of security investment (Gordon & Loeb, 2002).

The study uses a secondary analysis of an existing deidentified dataset collected from industrial control system and operational technology professionals. The data source is relevant because operational technology is a high-consequence environment in which trust, risk, control, and investment confidence are especially important. However, the argument extends beyond operational technology alone. Research on security operations centers shows that cyber deception remains underused in enterprise environments due to unclear use cases, limited empirical evidence, hesitancy toward active defense, vendor overpromising, and concerns about disrupting analyst decision-making (Reeves & Ashenden, 2023). The current study uses the operational technology dataset as the empirical anchor while interpreting the findings through cross-domain research on cyber deception, technology acceptance, security economics, analyst decision making, and risk communication.

2. Literature Background

2.1. Defensive Cyber Deception as an Investment Category

Defensive cyber deception has evolved beyond simple honeypots. Current taxon-

omies describe a broad set of techniques, including decoys, honeytokens, moving target defense, obfuscation, fake credentials, simulated assets, and adversary engagement mechanisms (Beltran-Lopez et al., 2025; Zhang & Thing, 2021). The investment case for these technologies differs from that of conventional perimeter tools because their value is often realized through signal quality rather than alert volume. A decoy interaction can be meaningful precisely because legitimate users should have no business touching the decoy.

Experimental and cognitive research supports the view that cyber deception operates, in part, through perception and decision-making. The Tularosa Study examined how cyber and psychological deception affected professional red-team participants and found that deception can alter attacker behavior and decision-making processes (Ferguson-Walter et al., 2019). Cranford et al. (2021) similarly argued for a cognitive theory of cyber deception, noting that cyber deception is a human decision-making problem in which deceptive signals alter beliefs under uncertainty. Reid et al. (2024) extended the discussion to ethics, arguing that defensive deception influences human cognition and behavior and therefore requires ethical and governance consideration.

From an investment standpoint, these findings matter because they show that deception technology is not only a technical artifact. It is a sociotechnical control that requires organizational confidence in the signal, in the implementation, and confidence that the capability can be governed safely. The United Kingdom National Cyber Security Centre's cyber deception trials reinforce this point. The trials involved 121 organizations, 14 commercial providers, and 10 product trials across environments including cloud and operational technology, and the NCSC reported that many organizations remain interested but uncertain about where to start (National Cyber Security Centre, 2025).

2.2. Trust, Risk, and Technology Acceptance

Technology adoption research provides a useful lens for understanding why technically plausible tools may still fail to diffuse. The Unified Theory of Acceptance and Use of Technology identifies performance expectancy, effort expectancy, social influence, and facilitating conditions as important determinants of technology acceptance and use (Venkatesh et al., 2003). Later work has reexamined UTAUT and emphasized that technology acceptance is not only a matter of tool characteristics but also of attitudes, context, support, and organizational conditions (Dwivedi et al., 2019). The later UTAUT extension also addressed consumer contexts and the role of experience in technology use (Venkatesh et al., 2012).

Defensive cyber deception is a particularly interesting case because adoption requires trust in something intentionally false. Professionals must believe that the deception artifacts are safe, that the alerts are meaningful, that the capability will not interfere with legitimate work, and that the organization can manage the ethical and operational boundaries. In enterprise security operations centers, Reeves and Ashenden (2023) found that adoption barriers include a lack of clear use

cases, limited empirical evidence, hesitancy toward active defense, vendor over-promising, and concern that deception could disrupt analyst decision-making. These are not merely technical barriers. They are trust and confidence barriers.

2.3. Business Confidence and Cybersecurity Investment under Uncertainty

Cybersecurity investments are difficult to evaluate because they often seek to prevent uncertain future losses rather than generate directly observable revenue. Gordon and Loeb (2002) showed that optimal information security investment depends on the relationships among vulnerability, expected loss, and the effectiveness of the investment. In practice, security leaders must also justify investment by demonstrating risk reduction, operational resilience, auditability, and improved decision quality. Defensive cyber deception can contribute to these outcomes by producing higher-confidence signals, enriching incident response, validating segmentation assumptions, and improving understanding of adversary behavior.

The business case, however, is weakened if the technology category is poorly understood. If decision-makers see deception as obsolete honeypots or a niche research tool, they may not perceive it as a mature investment category. If practitioners do not trust the technology, lack experience with it, or cannot explain the use case to executives, the technology may fail to move from pilot to program. Therefore, this paper uses the term investment confidence to link perceived value and security trust to the organizational conditions that precede investment decisions.

3. Research Model and Hypotheses

Figure 1 presents the research model. The model treats investment confidence as a practitioner-level perception that combines perceived business/security value and security trust. The model assumes that demographics may influence adoption, but that technology-specific perceptions should explain substantially more variance than formal education, general experience, or sector membership.

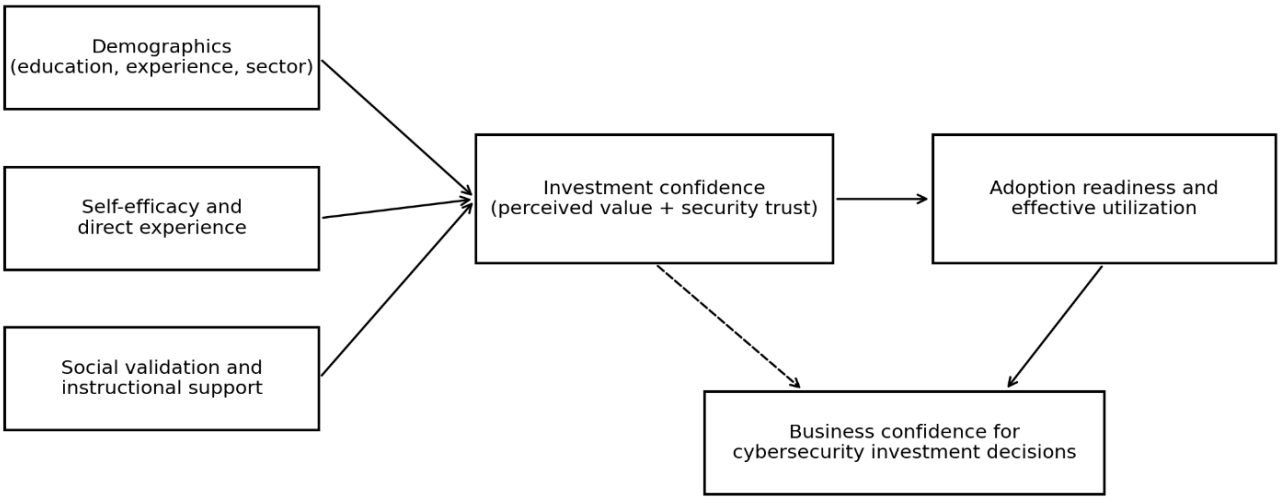

Figure 1. Investment confidence model for the adoption of defensive cyber deception.

Four research questions guided the analysis. RQ1 asked whether investment confidence, self-efficacy/direct experience, social validation, and instructional support were associated with adoption readiness and effective utilization. RQ2 asked whether perception-based predictors explained more variance in adoption readiness than demographics alone. RQ3 asked whether investment confidence remained significant after accounting for demographics and other perception-based predictors. RQ4 asked which variables predicted investment confidence itself.

The corresponding hypotheses were as follows. H1 stated that investment confidence, self-efficacy/direct experience, social validation, and instructional support would each be positively associated with adoption readiness. H2 stated that perception-based variables would explain significantly more variance in adoption readiness than demographics alone. H3 stated that investment confidence would remain a significant positive predictor in the full adoption model. H4 stated that self-efficacy/direct experience, social validation, and instructional support would significantly improve the prediction of investment confidence beyond demographics.

4. Materials and Methods

4.1. Data Source and Sample

The study used secondary analysis of a deidentified dataset collected for a completed dissertation on deception technology integration in manufacturing and critical infrastructure. The original study used a quantitative survey design and the Unified Theory of Acceptance and Use of Technology to examine the adoption of deception technology among industrial control system and operational technology professionals (Ward, 2025). The source dataset contained 317 records; 304 respondents consented to participate. After listwise deletion for the variables in the primary regression model, the complete-case sample was 264.

The original sampling frame targeted controls engineers, controls technicians, and cybersecurity or IT practitioners with at least two years of experience integrating information technology, including networks, servers, or firewalls, into ICS/OT environments. Recruitment occurred through a structured SurveyMonkey survey distributed through SurveySwap and LinkedIn, with respondents drawn from food and beverage manufacturing, consumer goods manufacturing, water/wastewater, and power generation settings.

Listwise deletion was used because the hierarchical regression models required the same observations across demographics-only and perception-augmented models. This approach preserved comparability of R-squared change tests and avoided shifting sample sizes across nested models. A descriptive comparison of retained respondents and excluded respondents with available demographic data did not indicate a meaningful demographic imbalance, although the excluded subgroup with complete demographic fields was small. Retained cases were 69.7% four-year degree and 30.3% graduate degree, while excluded cases with available

education data were 62.5% four-year degree and 37.5% graduate degree. Retained cases were also concentrated in the two-to-five-year experience group, 78.8%, similar to the excluded subgroup, 81.3%. Sector distributions varied modestly, but both groups were concentrated in food and beverage and consumer goods manufacturing.

4.2. Measures

Investment confidence was operationalized as the mean of four items: deception technology would make detection and response easier, deception technology is a good idea for enhancing cybersecurity, deception technology would enable cybersecurity tasks to be completed more quickly, and deception technology is secure. This composite corresponds to the original perceived risks and benefits composite in the dissertation dataset, rescaled as a mean. Adoption readiness and effective utilization were measured using the existing composite of ease of learning, ease of use, resource availability, organizational control, and positive experience. Self-efficacy/direct experience used the skill and prior-experience items. Social validation used the two social-influence items. Instructional support was measured as a single item reflecting whether instruction was available to help the respondent use deception technologies.

Investment confidence and adoption readiness/effective utilization were retained as separate constructs because they represent different points in the investment-adoption pathway. Investment confidence captures perceived value and security trust, meaning whether the capability appears worth organizational attention and resources. Adoption readiness/effective utilization captures perceived ability and conditions for use, meaning whether respondents believe the technology can be learned, controlled, resourced, and used positively in practice.

The original sample included both respondents with prior deception-technology experience and respondents without substantial prior experience. For that reason, the outcome should be interpreted as adoption readiness and perceived effective utilization rather than as an objective usage-intensity measure. The composite is appropriate across the full sample because the items address readiness and use-related perceptions, while direct prior experience was modeled separately through the self-efficacy/direct-experience predictor.

A measurement constraint should be noted. The self-efficacy/direct-experience scale had modest internal consistency and instructional support was measured with a single item. These variables were retained because self-efficacy, direct experience, and instructional availability are theoretically central to technology acceptance and investment confidence, but their coefficients should be interpreted as exploratory and construct-specific rather than as fully validated latent measurement estimates. The construct definitions, item mappings, and reliability estimates are summarized in Table 1.

4.3. Statistical Procedure

The analysis used descriptive statistics, Cronbach's alpha, pearson and spearman

correlations, and hierarchical ordinary least squares regression. Spearman correlations were included because the survey used an ordered Likert-type

Table 1. Construct operationalization.

Construct	Items	Interpretation	Reliability
Investment confidence	Q5, Q6, Q7, Q16	Perceived business/security value, speed, usefulness, and security trust	alpha = 0.728
Adoption readiness/effective utilization	Q9, Q10, Q13, Q15, Q18	Ease, resources, control, and positive adoption/use experience	alpha = 0.772
Self-efficacy/direct experience	Q8, Q17	Skill to implement/manage and prior experience	alpha = 0.616
Social validation	Q11, Q12	Influence from important peers and stakeholders	alpha = 0.734
Instructional support	Q14	Instructional availability	Single item
Demographics	Q2, Q3, Q4	Education (graduate-level degree relative to four-year degree), years of experience, and sector dummy controls	Controls

response scale. Education was coded as graduate-level degree = 1 and four-year degree = 0. Years of experience was modeled as an ordinal variable. Sector was entered through three dummy variables for consumer goods manufacturing, water/wastewater, and power generation, with food and beverage manufacturing serving as the reference category. Hierarchical regression compared a demographics-only model against a model that added investment confidence, self-efficacy/direct experience, social validation, and instructional support. Coefficient-level inference used HC3 robust standard errors to reduce sensitivity to heteroscedasticity. Tables 2-3 report unstandardized coefficients, HC3 robust standard errors, 95% confidence intervals, standardized betas, and p-values to support reproduction of the regression models. A second hierarchical regression model used investment confidence as the dependent variable to test whether social and capability factors predicted the perceived investability of defensive cyber deception. The education coefficient should therefore be interpreted as graduate-level degree relative to the four-year degree reference category, not as a separate education-only category. Sector coefficients should be interpreted relative to food and beverage manufacturing, which was the omitted reference sector.

5. Results

For transparency and to establish the coefficient-level results used throughout this section, Table 2 reports the full adoption-model coefficients, and Table 3 reports the full investment-confidence-model coefficients.

Table 2. Full adoption model coefficients with HC3 robust standard errors.

Predictor	b	HC3 SE	95% CI	beta	*p*
Intercept	−0.019	0.090	[−0.194, 0.157]		0.836
Graduate-level degree (ref. four-year degree)	0.101	0.077	[−0.050, 0.252]	0.052	0.189
Years of experience	0.058	0.059	[−0.058, 0.174]	0.037	0.326
Consumer goods manufacturing (ref. food and beverage)	−0.057	0.077	[−0.208, 0.094]	−0.031	0.456
Water/wastewater (ref. food and beverage)	0.084	0.126	[−0.164, 0.332]	0.020	0.507
Power generation (ref. food and beverage)	0.127	0.111	[−0.091, 0.346]	0.042	0.254
Investment confidence	0.259	0.073	[0.115, 0.402]	0.251	<0.001
Self-efficacy/direct experience	0.311	0.068	[0.178, 0.444]	0.415	<0.001
Social validation	0.102	0.068	[−0.030, 0.235]	0.125	0.130
Instructional support	0.177	0.051	[0.077, 0.276]	0.240	<0.001

Note. Education and sector predictors are dummy-coded. Graduate-level degree is compared with the four-year degree reference category. Consumer goods manufacturing, water/wastewater, and power generation are each compared with the food and beverage manufacturing reference sector.

Table 3. Full investment-confidence model coefficients with HC3 robust standard errors.

Predictor	b	HC3 SE	95% CI	beta	*p*
Intercept	0.267	0.154	[−0.034, 0.568]		0.082
Graduate-level degree (ref. four-year degree)	0.148	0.112	[−0.071, 0.366]	0.078	0.186
Years of experience	0.208	0.097	[0.018, 0.398]	0.137	0.032
Consumer goods manufacturing (ref. food and beverage)	0.025	0.106	[−0.181, 0.232]	0.014	0.810
Water/wastewater (ref. food and beverage)	0.016	0.200	[−0.376, 0.408]	0.004	0.937
Power generation (ref. food and beverage)	−0.293	0.206	[−0.696, 0.110]	−0.100	0.154
Self-efficacy/direct experience	0.154	0.074	[0.009, 0.300]	0.213	0.038
Social validation	0.214	0.089	[0.040, 0.388]	0.269	0.016
Instructional support	0.097	0.059	[−0.018, 0.212]	0.136	0.097

Note. Education and sector predictors are dummy-coded. Graduate-level degree is compared with the four-year degree reference category. Consumer goods manufacturing, water/wastewater, and power generation are each compared with the food and beverage manufacturing reference sector.

5.1. Descriptive Statistics and Reliability

Table 4 shows that average responses were positive across all constructs, but the standard deviations indicate substantial variation in confidence, self-efficacy, and support. This variation is analytically useful because it allows the secondary analysis to test whether investment confidence and related perception variables explain adoption readiness.

5.2. Bivariate Associations

All four perception-based predictors were positively associated with adoption

readiness. The strongest bivariate association was self-efficacy/direct experience, r = 0.697, $p < 0.001$. Investment confidence was also strongly associated with adoption readiness, r = 0.566, $p < 0.001$. Spearman correlations showed the same substantive pattern, supporting H1. The complete Pearson and Spearman results are reported in Table 5. As shown in Figure 2, self-efficacy/direct experience had the strongest bivariate association, while the remaining perception-based predictors showed associations of similar positive direction.

Table 4. Descriptive statistics for primary constructs.

Construct	N	Mean	SD	Min	Max
Adoption readiness/effective utilization	264	0.66	0.90	−3	3
Investment confidence	264	0.85	0.88	−3	3
Self-efficacy/direct experience	264	0.48	1.21	−3	3
Social validation	264	0.68	1.10	−3	3
Instructional support	264	0.80	1.23	−3	3

Table 5. Associations with adoption readiness and effective utilization.

Predictor	Pearson r	*p*	Spearman rho	*p*	H1 result
Investment confidence	0.566	<0.001	0.492	<0.001	Supported
Self-efficacy/direct experience	0.697	<0.001	0.610	<0.001	Supported
Social validation	0.559	<0.001	0.562	<0.001	Supported
Instructional support	0.567	<0.001	0.488	<0.001	Supported

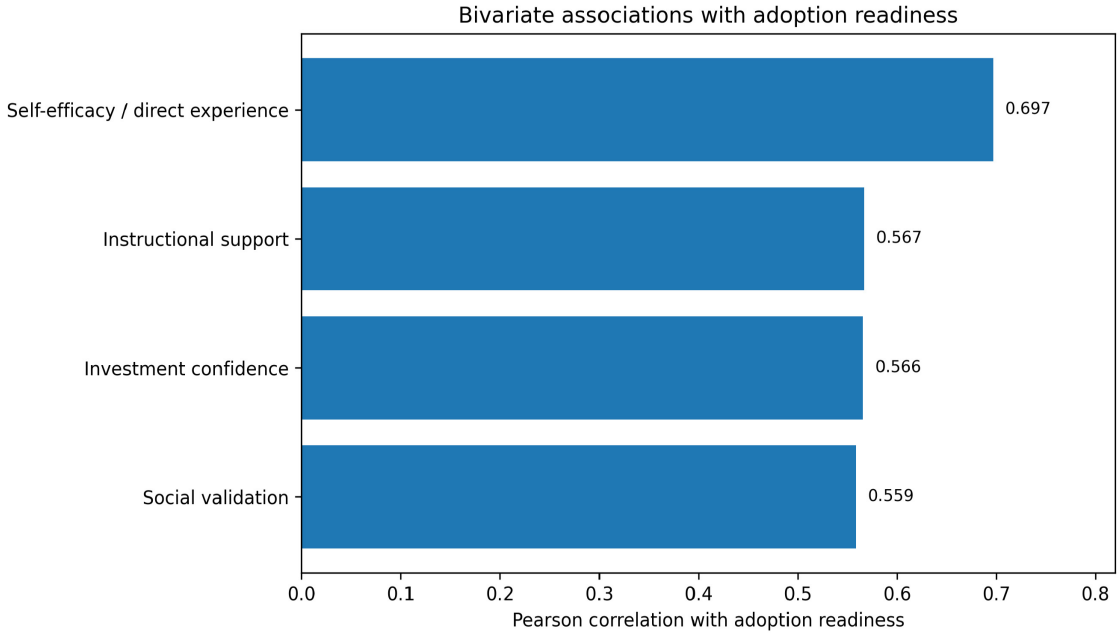

Figure 2. Bivariate associations with adoption readiness and effective utilization.

5.3. Hierarchical Regression Predicting Adoption Readiness

The demographics-only model did not meaningfully explain adoption readiness, R-squared = 0.026, F (5, 258) = 1.40, $p = 0.225$. When investment confidence, self-efficacy/direct experience, social validation, and instructional support were added, model fit improved substantially, R-squared = 0.639, adjusted R-squared = 0.626, F (9, 254) = 49.96, $p < 0.001$. The R-squared change was 0.613, F change(4, 254) = 107.78, $p < 0.001$. H2 was therefore supported. As shown in Figure 3, the perception-based model explained substantially more variance than the demographics-only model. Table 6 summarizes the nested-model statistics and the test of H2.

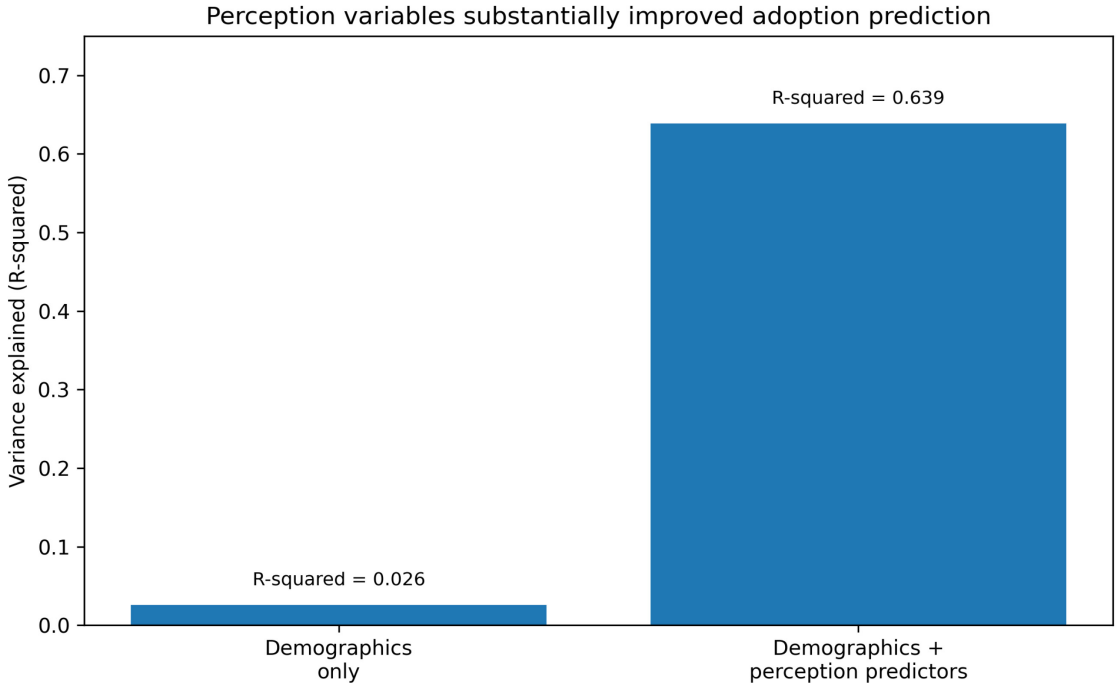

Figure 3. Variance explained by demographics alone compared with the full perception model.

Table 6. Hierarchical regression results for adoption readiness.

Model/Test	Specification	Primary statistic	*p* value	Interpretation
Demographics only	Graduate-level degree dummy, years of experience, and three sector dummies	R-squared = 0.026; F (5, 258) = 1.40	$p = 0.225$	Not significant
Full adoption model	Demographics plus investment confidence, self-efficacy/direct experience, social validation, and instructional support	R-squared = 0.639; adjusted R-squared = 0.626; F (9, 254) = 49.96	$p < 0.001$	Significant
Model improvement	Full model compared with demographics-only model	Delta R-squared = 0.613; F change (4, 254) = 107.78	$p < 0.001$	Supported

Note. Education was represented by one dummy variable: graduate-level degree = 1 and four-year degree = 0/reference category. Sector was represented by three dummy variables for consumer goods manufacturing, water/wastewater, and power generation; food and beverage manufacturing was the reference category. The five demographic parameters in the demographics-only model were the graduate-degree dummy, years of experience, and three sector dummies.

5.4. Full-Model Predictor Effects

Table 2 reports unstandardized coefficients, HC3 robust standard errors, 95% confidence intervals, standardized betas, and p-values for the full adoption model. H3 was supported because investment confidence remained a statistically significant predictor in the full model, b = 0.259, HC3 SE = 0.073, beta = 0.251, $p < 0.001$. Self-efficacy/direct experience was the strongest predictor, beta = 0.415, $p < 0.001$, and instructional support was also significant, beta = 0.240, $p < 0.001$. Social validation was positive but not statistically significant after the stronger predictors were included. Figure 4 visualizes the standardized beta coefficients for the main perception-based predictors.

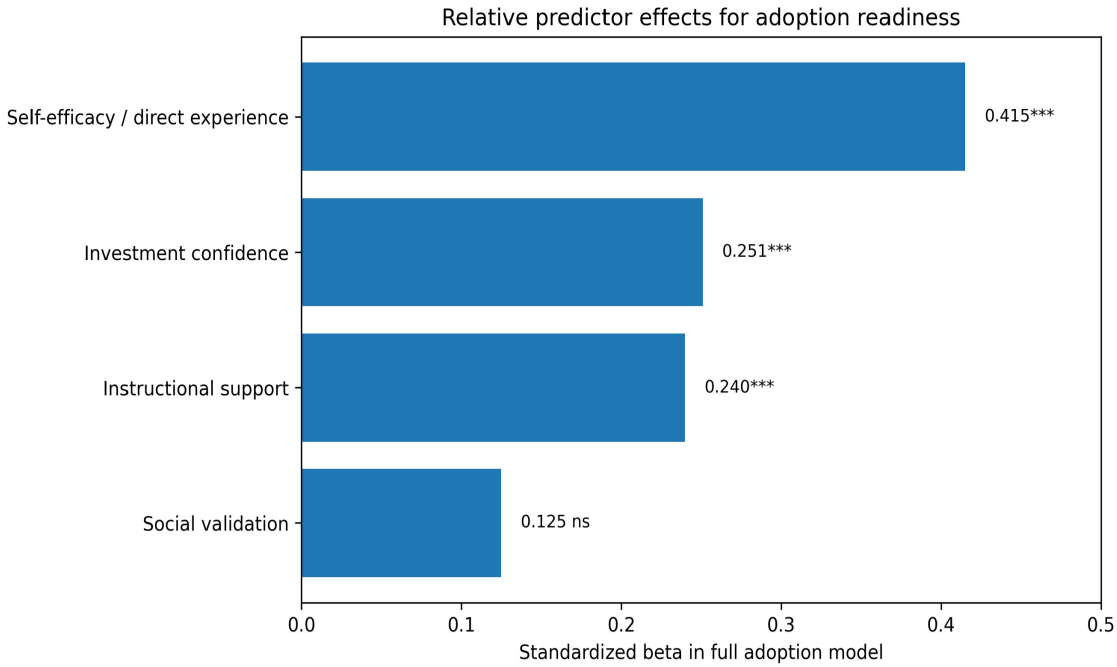

Figure 4. Standardized beta coefficients for the main perception predictors in the full adoption model.

5.5. Predicting Investment Confidence

A second hierarchical regression used investment confidence as the dependent variable. The demographics-only model explained 4.6 percent of variance, F (5, 258) = 2.48, $p = 0.032$. Adding self-efficacy/direct experience, social validation, and instructional support increased explained variance to R-squared = 0.291, adjusted R-squared = 0.269, F (8, 255) = 13.11, $p < 0.001$. The R-squared change was 0.245, F change (3, 255) = 29.44, $p < 0.001$. Table 3 reports the full coefficient results. In the full model, self-efficacy/direct experience, b = 0.154, beta = 0.213, $p = 0.038$, and social validation, b = 0.214, beta = 0.269, $p = 0.016$, were significant predictors of investment confidence. Instructional support was positive but not statistically significant at the 0.05 level, beta = 0.136, $p = 0.097$. H4 was partially supported. The complete coefficient estimates for the investment-confidence model are reported in Table 3.

6. Discussion

The findings support a data-driven investment narrative. Defensive cyber deception acceptance was not primarily explained by formal education, years of experience, or sector. Instead, adoption readiness was explained by investment confidence, self-efficacy/direct experience, and instructional support. The full perception model explained nearly two-thirds of the variance in adoption readiness, while demographics alone explained less than three percent. This suggests that organizations evaluating deception technology should focus less on whether the workforce has generic technical credentials and more on whether practitioners understand the use case, trust the security value, and feel capable of using the capability safely.

6.1. Investment Confidence Is a Practical Precondition for Funding

The investment implication is straightforward. A cybersecurity capability is unlikely to receive durable funding if the workforce cannot articulate why it creates value, why it is trustworthy, and how it can be operated without creating new risk. Investment confidence, therefore, operates as a bridge between technical potential and business decision-making. In this dataset, investment confidence significantly predicted adoption readiness even after controlling for self-efficacy, social validation, instructional support, education, experience, and sector. This finding supports the idea that perceived value and security trust are not soft concerns. They are measurable predictors of whether a security capability is likely to be accepted as a real operational investment.

6.2. Deception Investment Should Be Framed as Signal Confidence, Not Tool Replacement

A recurring adoption problem is that deception technology may be misunderstood as a replacement for other controls or as an isolated honeypot project. The investment case is stronger when deception is framed as an additive signal of confidence. Firewalls, endpoint detection, asset inventory, segmentation, identity security, vulnerability management, and monitoring remain necessary. Deception adds value by enabling high-confidence interactions that can reveal reconnaissance, credential misuse, lateral movement, or unauthorized access to assets that legitimate users should not touch. This framing is consistent with SOC research emphasizing high-fidelity, low-volume alerting as a reason deception may help overwhelmed defenders (Reeves & Ashenden, 2023). Later SOC deployment research likewise emphasizes operational integration and implementation fit (Reeves, 2025).

6.3. Investment under Uncertainty Requires Governance and Evidence

The results also imply that investment confidence requires evidence. Business leaders may reasonably ask whether deception platforms will generate useful de-

tections, whether they will increase false positives, whether they can be governed ethically, and whether they will fit analyst or operator workflows. The NCSC cyber deception trials show that many organizations are interested in deception but need guidance, real-world evidence, and reassurance about safety and effectiveness (National Cyber Security Centre, 2025). Prior control-mapping and readiness work similarly argue that deception must be translated into governance, monitoring, response, audit evidence, and workforce capability before it becomes a mature cybersecurity program element (Ward, 2026a, 2026d). These requirements align with IEC 62443-2-1 asset-owner security programs and the NIST Cybersecurity Framework 2.0 Govern function (International Electrotechnical Commission, 2024; National Institute of Standards and Technology, 2024).

6.4. IT and OT Differences

The study's empirical data came from ICS/OT professionals, so the safety-sensitive interpretation is important. In OT environments, perceived control and trust matter because poor implementation can disrupt physical processes, confuse operators, or introduce unacceptable change-control issues. In enterprise IT and SOC environments, the emphasis may be different. The central concerns may include analyst workflow, alert confidence, the legitimacy of active defense, and integration with existing monitoring tools. Across both domains, however, the same investment-confidence pattern appears relevant: professionals need to understand what deception is, trust the signal, and believe the organization can act on it. NIST OT guidance similarly emphasizes safety, reliability, availability, and process integrity (National Institute of Standards and Technology, 2023), while sector-specific water research demonstrates passive, staged, safety-aware deception design (Ward, 2026b).

7. Practical Implications

For cybersecurity leaders, the findings suggest four practical steps. First, evaluate deception technology using investment criteria that include signal fidelity, response enrichment, governance evidence, workflow integration, and operational risk. Second, fund training and lab exposure before expecting professionals to support production deployment. Self-efficacy/direct experience were the strongest predictors of adoption readiness, suggesting that hands-on familiarity may be more persuasive than vendor claims or policy language alone. Third, treat social validation as part of the investment process. The investment-confidence model showed that social validation significantly predicted investment confidence, suggesting that peer and stakeholder endorsement can shape perceptions of credibility. Fourth, insist on evidence-based pilot designs. A pilot should document expected use cases, decoy ownership, monitoring pathways, response procedures, false-positive criteria, and investment evaluation metrics. This emphasis also aligns with a workforce-readiness model centered on governance literacy, OT context awareness, deception design, intelligence translation, and response inte-

gration (Ward, 2026c).

For vendors, the findings suggest that market adoption will depend on clarity and credibility. The category is still poorly understood, and many organizations do not know where to start. Vendors that frame deception as a measurable, governed, evidence-producing capability may be better positioned than vendors that frame it as a generic attack-trapping tool. For boards and executives, the key question is not whether deception is interesting. The key question is whether it reduces uncertainty, improves decision confidence, and supports defensible cybersecurity investment decisions.

8. Limitations and Future Research

This study has limitations. The dataset was originally collected for dissertation research focused on ICS/OT professionals in manufacturing and critical infrastructure. The results may not generalize to all enterprise IT, cloud, or SOC environments. The analysis is cross-sectional, so it cannot establish causal direction. The investment-confidence construct is a secondary operationalization built from perceived value and security trust items rather than a direct survey of executives or budget owners. The data are self-reported and may be affected by response bias, familiarity bias, or social desirability.

The measurement model also has limitations. Self-efficacy/direct experience showed modest internal consistency, and instructional support was measured with a single item. These variables were retained because they directly represent experience, capability, and support mechanisms central to the research questions, but future studies should use multi-item measures and confirmatory measurement models to strengthen construct validity.

Future research should test the model with enterprise security operations center analysts, cloud security teams, managed security providers, and business decision makers. A useful next study would use a vignette-based experiment comparing traditional alerts, deception alerts, and enriched deception alerts to measure trust, escalation confidence, perceived business value, and willingness to fund a pilot. Another useful study would compare organizations that have deployed deception technology with those that have not, focusing on whether hands-on exposure to deception technology changes investment confidence.

9. Conclusion

Defensive cyber deception is often evaluated as a technical capability, but the investment decision is also psychological and organizational. This secondary analysis found that perception-based variables explained substantially more of the variance in adoption readiness than demographics alone. Investment confidence, self-efficacy/direct experience, and instructional support were significant predictors of adoption readiness and effective utilization. Investment confidence itself was predicted by self-efficacy and social validation. These results suggest that organizations seeking to adopt defensive cyber deception should not begin with tool

procurement alone. They should build confidence through clear use cases, hands-on experience, trust-building evidence, governance, and safe operational design. In business terms, deception becomes investable when practitioners can explain what it detects, why the signal is trustworthy, how it will be controlled, and how it improves cybersecurity decision-making under uncertainty.

Ethics Statement

This manuscript uses secondary analysis of an existing deidentified dissertation dataset. No new participants were recruited, and no new human-subject data were collected.

Data Availability

The deidentified dataset and analysis outputs may be made available by the author upon reasonable request, subject to applicable institutional and ethical restrictions.

Generative AI Disclosure

Generative AI assistance using Grammarly was used to support formatting and editing. The author reviewed, revised, and approved the manuscript and is responsible for the accuracy, interpretation, and source attribution.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Beltran-Lopez, P., Gil Perez, M., & Nespoli, P. (2025). Cyber deception: Taxonomy, state of the art, frameworks, trends, and open challenges. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2025.3594788

Cranford, E. A., Gonzalez, C., Aggarwal, P., Tambe, M., Cooney, S., & Lebiere, C. (2021). Towards a cognitive theory of cyber deception. Cognitive Science, 45(7), e13013. https://doi.org/10.1111/cogs.13013

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2019). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. Information Systems Frontiers, 21(3), 719-734. https://doi.org/10.1007/s10796-017-9774-y

Ferguson-Walter, K. J., Shade, T. B., Rogers, A. V., Niedbala, E., Trumbo, M. C. S., Nauer, K. S., Divis, K. M., Jones, A., Combs, A., & Abbott, R. G. (2019). The Tularosa Study: An experimental design and implementation to quantify the effectiveness of cyber deception. Proceedings of the 52nd Hawaii International Conference on System Sciences. https://hdl.handle.net/10125/59938

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457. https://doi.org/10.1145/581271.581274

IBM. (2025). Cost of a Data Breach Report 2025. https://www.ibm.com/reports/data-breach

International Electrotechnical Commission. (2024). IEC 62443-2-1:2024: Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners. https://webstore.iec.ch/en/publication/62883

National Cyber Security Centre. (2025). Cyber deception trials: What we have learned so far. https://www.ncsc.gov.uk/blog-post/cyber-deception-trials-what-weve-learned-so-far

National Institute of Standards and Technology. (2023). Guide to operational technology (OT) security (NIST Special Publication 800-82 Revision 3). https://doi.org/10.6028/NIST.SP.800-82r3

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29

Reeves, A., & Ashenden, D. (2023). Understanding decision making in security operations centres: Building the case for cyber deception technology. Frontiers in Psychology, 14, 1165705. https://doi.org/10.3389/fpsyg.2023.1165705

Reeves, A. (2025). Deploying cyber deception in a SOC. Proceedings of the 58th Hawaii International Conference on System Sciences. https://hdl.handle.net/10125/109838

Reid, I., Okeke-Ramos, A., & Serafin, M. (2024). Exploring the ethics of cyber deception technologies for defensive cyber deception. In P. Bednar, J. Kavrestad, E. Bergstrom, M. Rajanen, H. V. Hult, A. M. Braccini, A. S. Islind, & F. Zaghloul (Eds.), Proceedings of the 10th International Conference on Socio-Technical Perspectives in Information Systems (pp. 140-148). CEUR Workshop Proceedings. https://ceur-ws.org/Vol-3857/paper9.pdf

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1), 157-178. https://doi.org/10.2307/41410412

Ward, D. (2025). Enhancing security: A comprehensive study on deception technology integration in manufacturing and critical infrastructure [Doctoral dissertation, University of the Cumberlands]. ProQuest Dissertations & Theses.

Ward, D. (2026a). Operationalizing deception technology in ICS/OT: A control mapping framework for critical infrastructure cybersecurity. International Journal of Soft Computing and Engineering, 16(3), 1-9. https://doi.org/10.35940/ijsce.C3723.16030726

Ward, D. (2026b). Deception architecture for water and wastewater operational technology environments. International Journal of Engineering Research & Technology, 15(6). https://doi.org/10.5281/zenodo.20745399

Ward, D. (2026c). A workforce readiness model for deception technology in ICS and OT cybersecurity programs. International Research Journal of Engineering and Technology, 13(6), 610-614. https://www.irjet.net/archives/V13/i6/IRJET-V13I0693.pdf

Ward, D. (2026d). A deception readiness index for ICS and OT cybersecurity programs. International Journal for Research in Applied Science & Engineering Technology, 14(VI), 2401-2406. https://doi.org/10.22214/ijraset.2026.83810

Zhang, F., & Thing, V. L. L. (2021). Three decades of deception techniques in active cyber defense: Retrospect and outlook. Computers & Security, 106, 102288. https://doi.org/10.1016/j.cose.2021.102288