The Cyber Risk Gap: What DFS Guidance Reduces — and What It Doesn't

Special Report

DFS has issued a clear warning: the threat environment has shifted. Guidance alone, however, does not quantify how much risk an organization is carrying, which controls will reduce it most, or where to concentrate effort first. This report addresses those questions directly — translating DFS recommendations into scenario-based, quantified business risk and identifying the specific interventions that produce material reductions in exposure.

Executive Summary

Five findings every financial sector executive needs to understand about cyber risk in a heightened threat environment.

DFS Controls Help — But Don't Close the Gap

DFS-aligned controls materially improve organizational resilience across all sectors. However, the likelihood of industry attacks does not change. Residual risk of attacks on individual companies remains elevated across all top risk scenarios.

Risk Is Non-Linear

Small declines in control execution can produce disproportionately large increases in attack success and loss severity. The relationship between controls and outcomes is asymmetric and compounding.

Execution — Not Presence — Determines Outcomes

Most financial institutions already have the controls DFS references. What determines risk is how consistently and effectively those controls perform under pressure, and how they are prioritized, not whether they exist on paper.

Not All Controls Reduce Risk Equally

Targeted prioritization of attack-path failure points produces greater risk reduction than broad control improvement. Ransomware shows the largest incremental benefit; third-party and state-sponsored risks show the least.

Residual Risk Requires Ongoing Forecasting

Even after DFS alignment and targeted prioritization, material residual risk remains. Organizations require continuously updated, quantified risk forecasts — not static guidance — to make defensible decisions in today's heightened risk environment.

The Non-Linear Risk Problem: Consistency Matters

Key Finding

In today's heightened threat environment, **control effectiveness erodes unevenly and sometimes accelerates under pressure, while the impact expands disproportionately.**

> "In some AI-driven attack paths, traditional controls are no longer meaningfully effective."
>
> *Charlene Deaver-Vazquez*

The Core Risk Dynamic

The relationship between controls and outcomes is increasingly **non-linear, asymmetric, and compounding**. Small declines in control performance can enable significantly larger increases in attack success and loss severity. ***(This is why consistency matters.)***

⚠ In a heightened threat environment, risk can escalate disproportionately even when control maturity improves if controls are applied inconsistently.

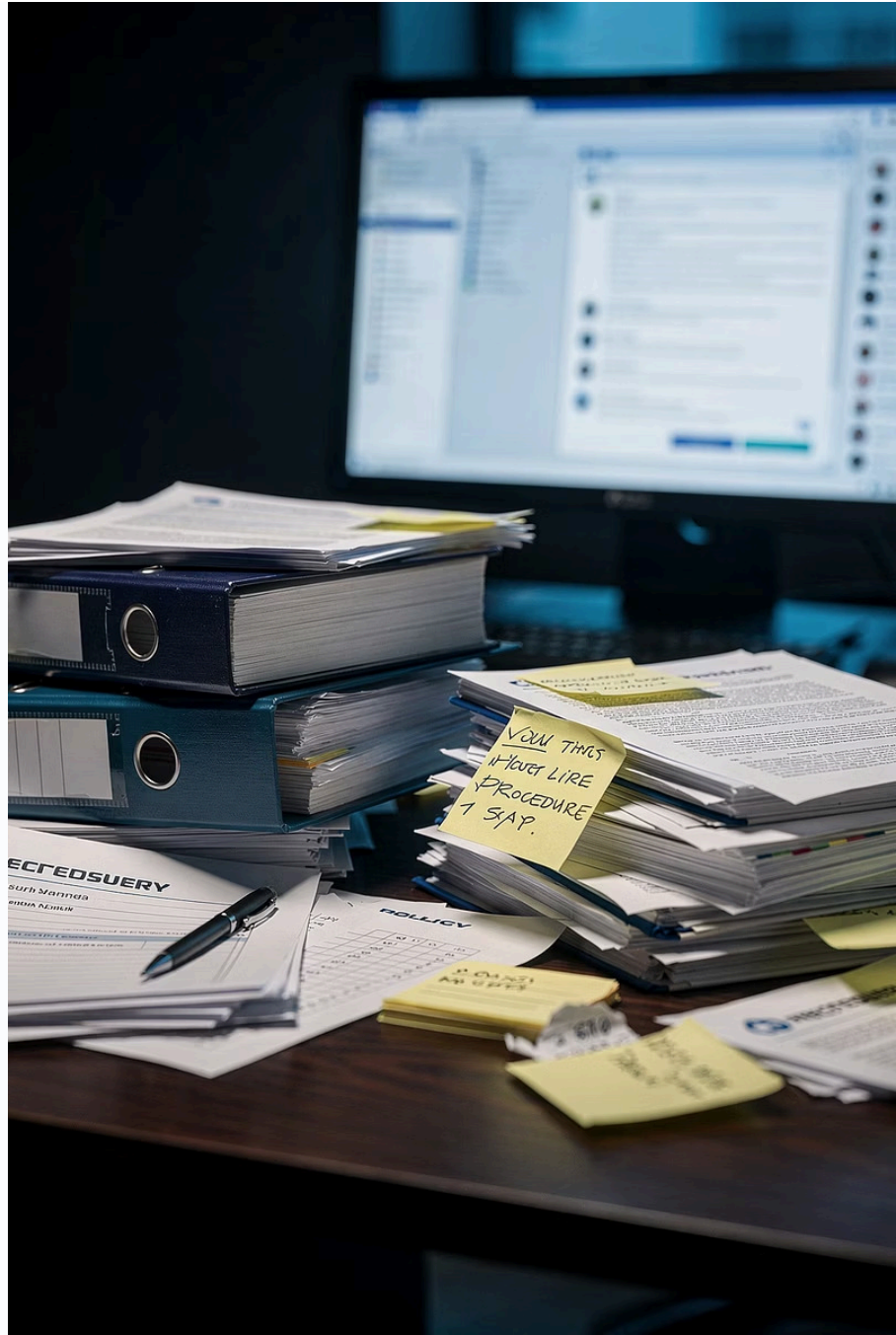
Without this understanding, financial firms risk:

- Overconfidence in control maturity
- Blind spots in detection and response
- No clear view of residual exposure

Controls Exist — Execution Under Pressure Is What Fails

The controls DFS references — vulnerability management, MFA, monitoring, third-party oversight — are not new. Most financial institutions already have them. What's missing is consistent, disciplined execution. That gap is where risk lives.

In a heightened threat environment, controls that performed adequately at lower threat levels begin to show measurable degradation — not because they were removed, but because attack velocity, adaptability, and AI-assisted execution have outpaced the assumptions under which those controls were designed. Organizations that apply uniform urgency across all controls will distribute effort inefficiently and fail to address the interventions with the greatest risk-reduction potential. The **approach should be outcome-focused: identify the points at which attacks transition into material business events, and concentrate remediation there first.**



What Organizations Need

Quantified Scenario-Based Risk

Organizations require risk analysis expressed as specific, plausible business events — not abstract threat categories. Each scenario must carry a quantified likelihood and estimated financial impact so that leadership can assess exposure in terms that support investment and prioritization decisions.

Continuously Updated Threat Context

The threat environment changes faster than annual assessments can capture. Organizations need risk forecasts that reflect the most recent 30–90 days of observed attack activity, geopolitical developments, and AI-driven threat evolution — recalculated on a regular cadence.

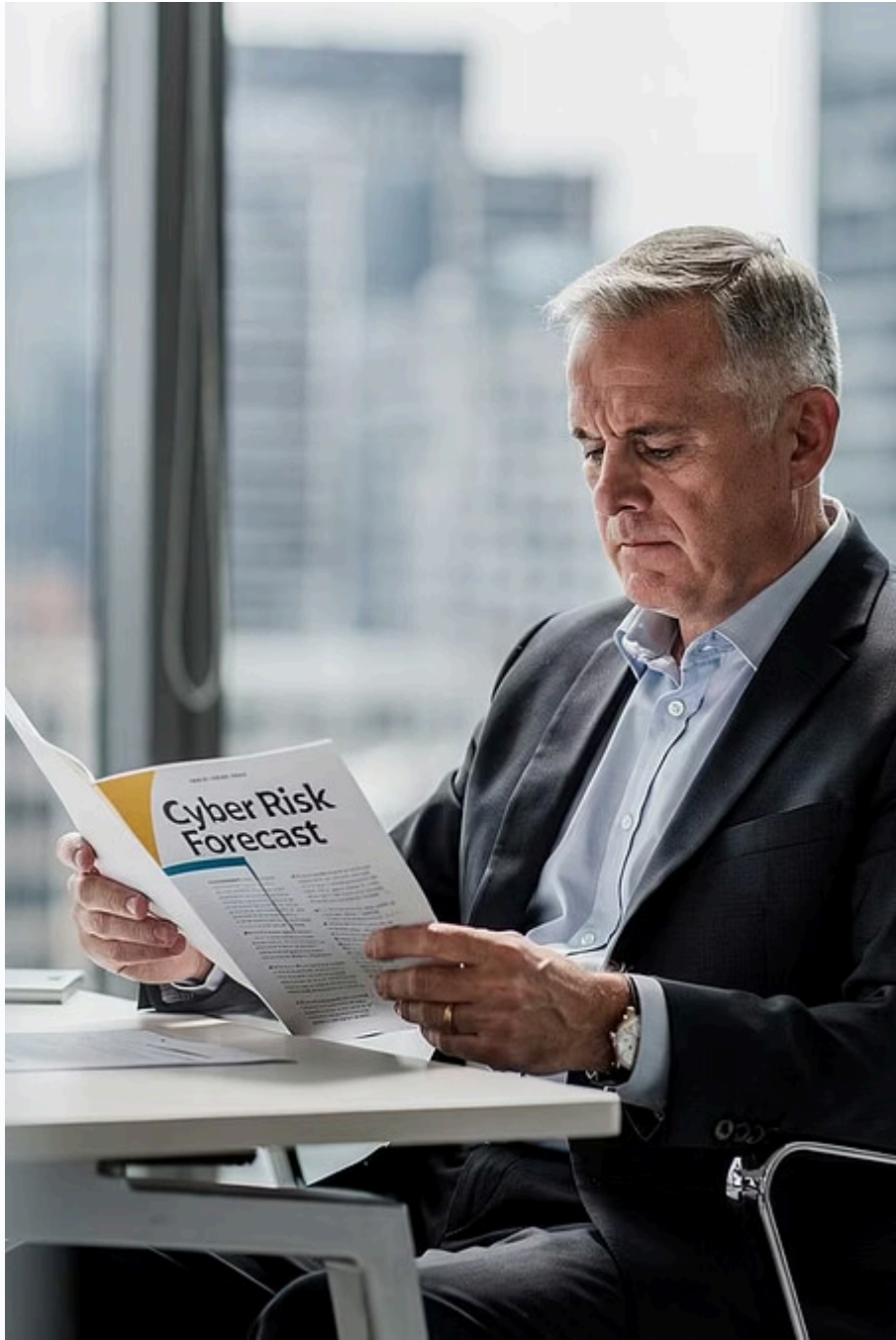
Control Effectiveness Measurement — Not Just Presence

Knowing which controls are deployed is insufficient. Organizations need a **measurable view of how effectively those controls are performing under current threat conditions** — and where execution gaps are creating residual exposure that static checklists cannot reveal.

A Prioritization Framework Tied to Outcomes

terms of scenarios Organizations need a structured approach to identifying which interventions will produce the greatest reduction in expected loss — and which represent necessary but limited improvements — so that effort and investment are concentrated where they materially change outcomes.

Financial sector organizations require cyber risk analysis that translates complex threat data into clear, quantified, scenario-based insights — enabling executives to understand exposure, prioritize responses, and make defensible decisions under changing conditions.



DFS Guidance Overview

DFS defines a **"heightened cybersecurity threat environment"** as one in which cyber risks are significantly elevated and likely to affect information systems, nonpublic information, or operations.

Contributing Factors: Geopolitical events and technological developments, such as Frontier AI models.

Three Control-Oriented Areas

1. **Reducing the attack surface** — remediating known exploited vulnerabilities, restricting MFA enrollment changes, using phishing-resistant MFA, segmenting networks, reviewing cloud configurations, and conducting privileged access reviews
2. **Improving threat detection and readiness** — up-to-date detection/prevention tools, logging and alerting, threat intelligence, alerting personnel to social engineering, and validating third-party code
3. **Improving resilience and response** — testing backups, reviewing operational resilience procedures, planning communications during disruption, confirming critical OT continuity, and monitoring financial transactions

Reframing DFS Guidance as Business Scenarios

DFS organizes its guidance around controls and threat vectors, but executives make decisions based on scenarios and business impact. The table below reframes DFS focus areas in terms of scenarios.

Top Sector Risks	DFS Guidance Applied	Implied Controls
Ransomware & Data Extortion	Expeditiously remediate known exploited vulnerabilities; ensure detection and response controls are in use and acting on alerts; capture and analyze logs; test backup integrity, immutability, and restorability; review and test incident response and business continuity procedures.	Centralized vulnerability management & patch SLA enforcement; IDS/IPS; Logging & monitoring (SIEM/XDR); Endpoint Detection & Response (EDR); Backup integrity checks (immutable/offline); Incident Response Plan & tabletop exercises; Business Continuity & DR testing.
Business Email Compromise (BEC) & Fraud	Restrict MFA enrollment and changes; implement phishing-resistant MFA; alert personnel to social engineering threats; establish verification procedures for communications and transactions; monitor anomalous financial activity.	MFA (all users); Email security gateway; DMARC/DKIM/SPF configuration; Security awareness & phishing simulation program; Transaction Anomaly Detection / Fraud Analytics; Collaboration platform controls.
Third-Party & Supply-Chain Attacks	Enhance monitoring and validation of third-party code, applications, permissions, and practices; engage critical third-party providers to validate readiness; review cloud configurations; enforce least privilege and limit interconnected exposure.	Vendor risk assessments; Contractual security requirements; Continuous vendor monitoring; MSP/MSSP remote access controls; Software Supply Chain Security (SBOM validation, code signing); Cloud Security Posture Management (CSPM) / SaaS Security Assessment; Managed CRM/ERP SaaS controls.
State-Sponsored Banking Intrusions & Crypto Heists	Ensure monitoring, logging, and detection controls are current and acted upon; leverage threat intelligence; conduct privileged access reviews; segment networks; validate cloud and system configurations to reduce exposure to advanced and targeted threats.	Threat intelligence integration & continuous monitoring; Logging & monitoring (SIEM/XDR); IDS/IPS; Privileged Access Management (PAM); Privileged Session Recording; Role separation for admins; Network segmentation; Zero Trust Network Access (ZTNA); Cloud Security Posture Management (CSPM).

Why This Matters: The Scenario Gap

What Executives Need to Know

- How actual exposure is changing
- Which scenarios are becoming more likely or more severe
- What residual risk remains after recommended actions are applied
- Which actions will materially reduce risk

The Limitation of DFS Guidance Alone

DFS provides a useful defensive-control framework, but it does not answer those questions on its own. **Only a scenario-based view can translate a heightened threat environment into decision-useful business exposure.**

Executives need more than control status—they need to know how changes in threat are shifting actual exposure. Addressing that question requires measurable analysis of control effectiveness, threat conditions, and scenario-level business impact.

What We've Been Measuring

Since Q4 2025, cyber risk was analyzed and quantified across multiple industries. In Q1 2026, the analysis shifted to sector-specific modeling focused on business-level risk.

Business Profile Modeling

Three characteristics that influence attacker targeting decisions were identified and modeled across all 27 combinations, representing the full spectrum of business risk profiles within each sector.

Control Effectiveness Tracking

Baseline controls and control-strength assumptions were established for each profile, compared against real-world observations, and adjusted to reflect current operating conditions.

AI-Driven Attack Analysis

The analysis tracks the effect of AI-driven attacks on control erosion and geopolitical conditions that elevate risk across the financial sector — factors that static guidance does not capture.

Quantifying DFS Recommendations: Methodology

For each business type, baseline controls, maturity, and effectiveness have been established and applied through a standardized business profile framework to model how operating conditions affect targeting and risk. DFS recommendations are measured against an average baseline measure of resistance. We begin measuring from a baseline resilience of 50%/50% meaning every business is equally at risk. To this starting point, the DFS recommendations are applied.

Key Terminology

- **Industry Attack Probability** — the likelihood that a sector-level attack scenario will occur within the 30-, 60-, or 90-day forecast period
- **Company Resilience** — a composite measure of an organization's resistance under current control conditions**,** reflecting control effectiveness, operational defenses, and execution quality. The probability of successfully withstanding an attack.
- **Chance of Business Impact** — the conditional probability that the organization will experience a material impact because sector-level attacks are occurring.
- **Company Risk of Attack** — the probability that the attack scenario will materially affect the business **within the forecast period 30-60-90 days.**

Why Controls Don't Move Risk Equally

⚠ Business resilience can improve after applying DFS recommendations while company's risk of attack remains high and the residual risk stays material.

That is because **strengthening controls can improve resistance, but it does not reduce risk in equal measure** when:

- Attack activity is accelerating
- Attacker methods are adapting
- Conditions that drive loss remain elevated

External threat pressure is increasing faster than most organizations can strengthen the internal factors that limit impact. Some attacks will succeed, and some impacts cannot be fully prevented.

Key Findings Across All Sectors

Before examining the sector data, the cross-sector analysis reveals three consistent patterns.

What the Numbers Show

- **Ransomware** remains the highest-risk scenario across all three sectors, with forecast likelihood of 81–100% and residual scenario likelihood of 25–41% after DFS alignment.
- **BEC & Fraud** and **Third-Party** risks show moderate improvement but persistent residual exposure due to human-process and vendor dependency factors.
- **State-Sponsored Intrusions** show the smallest absolute residual likelihood but remain meaningful given advanced attacker capability.
- **ACRMI** improves by 9–20 percentage points across all scenarios after DFS alignment — but attack likelihood does not move.

The Consistent Pattern

Controls Improve, Threat Doesn't Move — Across every sector and scenario, DFS-aligned controls raise resistance. The forecast threat environment remains unchanged.

Residual Risk Is Material in Every Sector — No sector achieves low residual risk after DFS alignment. All organizations must plan for material exposure that controls cannot eliminate.

Sector Differences Are in Degree, Not Direction — Retail banking, FinTech, and Investment Management face the same top risks in the same order. The differences lie in exposure profile, attractiveness, and maturity — not in which threats matter most.

Sector Risk Analysis: DFS Alignment Outcomes

Covers: Retail & Commercial Banking · FinTech · Investment & Wealth Management

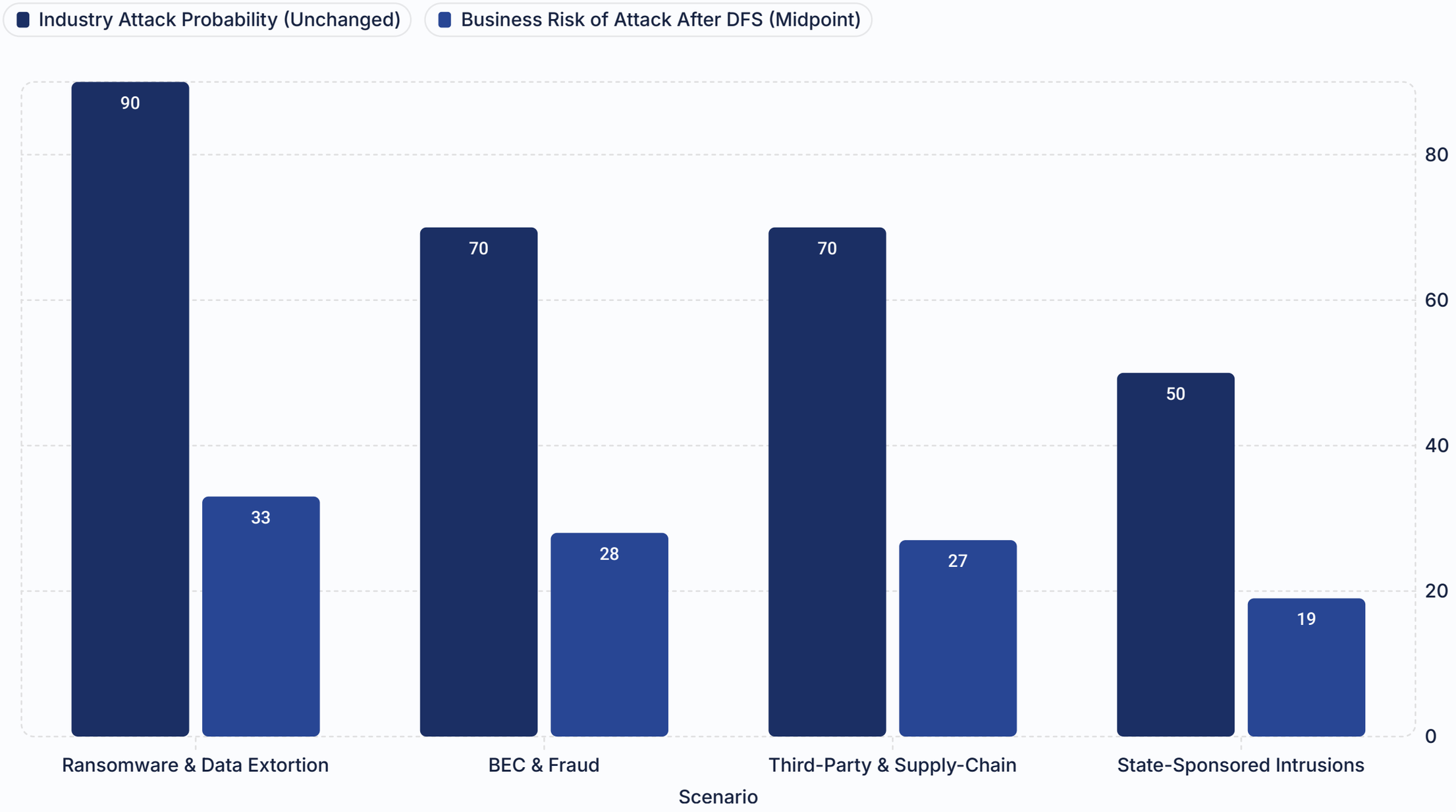
DFS-aligned controls produce measurable improvements in company resilience across all four top risk scenarios. Residual business risk remains material in every case — because the probability of industry attack stays elevated and control improvements do not translate into proportional reductions in business risk of attack or expected business impact.

Top Risk	Industry Attack Probability	Business Resilience	Resilience After DFS	Chance of Business Impact (After DFS)	Residual Business Risk of Attack (After DFS)	Residual Risk Level	Why Risk Remains Material (All Sectors)
Ransomware & Data Extortion	Very High (81–100%)	50%	~59–70%	~30–41%	~25–41%	Elevated	Sustained **attack pressure across all sectors exceeds what improved controls can offset**. Likelihood is effectively near-certain; resistance improves but residual exposure remains elevated.
BEC & Fraud	High (61–80%)	50%	~56–64%	~36–44%	~22–35%	Persistent	**Social engineering, impersonation, and transaction workflow manipulation remain difficult to fully suppress** across retail banking, FinTech, and wealth management despite DFS-aligned improvements.
Third-Party & Supply-Chain Attacks	High (61–80%)	50%	~58–68%	~32–42%	~20–34%	Elevated	Vendor ecosystems, shared platforms, and software reuse expose all three sectors to **risk that extends beyond direct organizational control a**fter DFS uplift.
State-Sponsored Intrusions & Crypto Heists	Moderate (41–60%)	50%	~58–68%	~32–43%	~13–26%	Meaningful	Advanced attacker capability, stealth, ge**opolitical targeting, and APT persistence** maintain residual exposure across all sectors despite control improvements.

The Gap DFS Cannot Close: Industry Attack Probability vs. Business Risk of Attack After DFS

Across all three sectors and all four top risk scenarios, DFS-aligned controls meaningfully reduce the business-level risk of attack — but the gap between industry attack probability (which does not change) and residual business risk of attack (after DFS) remains substantial. This is the residual risk organizations must plan for.

Industry Attack Probability vs. Business Risk of Attack After DFS (Midpoint Estimates)



Industry attack probability reflects sector-level threat conditions and does not change with organizational controls.

Targeting the Controls That Actually Change Outcomes

Not all controls reduce risk equally — focus on the points where attacks become business-impacting events.

Improving control effectiveness does not translate into proportional risk reduction when external threat pressure remains high. The framework identifies the specific control points that determine whether an attack progresses to a material outcome.

Critical Attack-Path Control Points

- Privilege escalation and administrative control
- Lateral movement across systems and environments
- Attack objective execution (encryption, fraud, exfiltration)
- Recovery failure or containment delay

Why This Produces Greater Risk Reduction

Outcome-Focused

Controls prioritized by their ability to prevent attacks from becoming material events, not just improve defensive posture.

Nonlinear Impact

Eliminating a single high-impact failure point can remove multiple high-loss scenarios, compressing the upper tail of risk.

Structural Exposure Reduction

Reduces the number of viable pathways to material impact, not just the likelihood within each pathway.

Incremental Effectiveness by Risk Category

Risk Category	Incremental Impact of Targeted Controls
Ransomware & Data Extortion	Greatest — discrete, controllable execution pathways
BEC & Fraud	Moderate — disrupts execution but cannot eliminate human decision risk
Third-Party & Supply-Chain	Limited — external systems and indirect control boundaries
State-Sponsored Intrusions	Limited — advanced adversaries retain multiple adaptive pathways

Effective cyber risk reduction is not driven by improving all controls equally — it is achieved by prioritizing the controls that prevent attacks from becoming business-impacting events.

DFS Guidance vs. Targeted Control Prioritization — Outcome Comparison

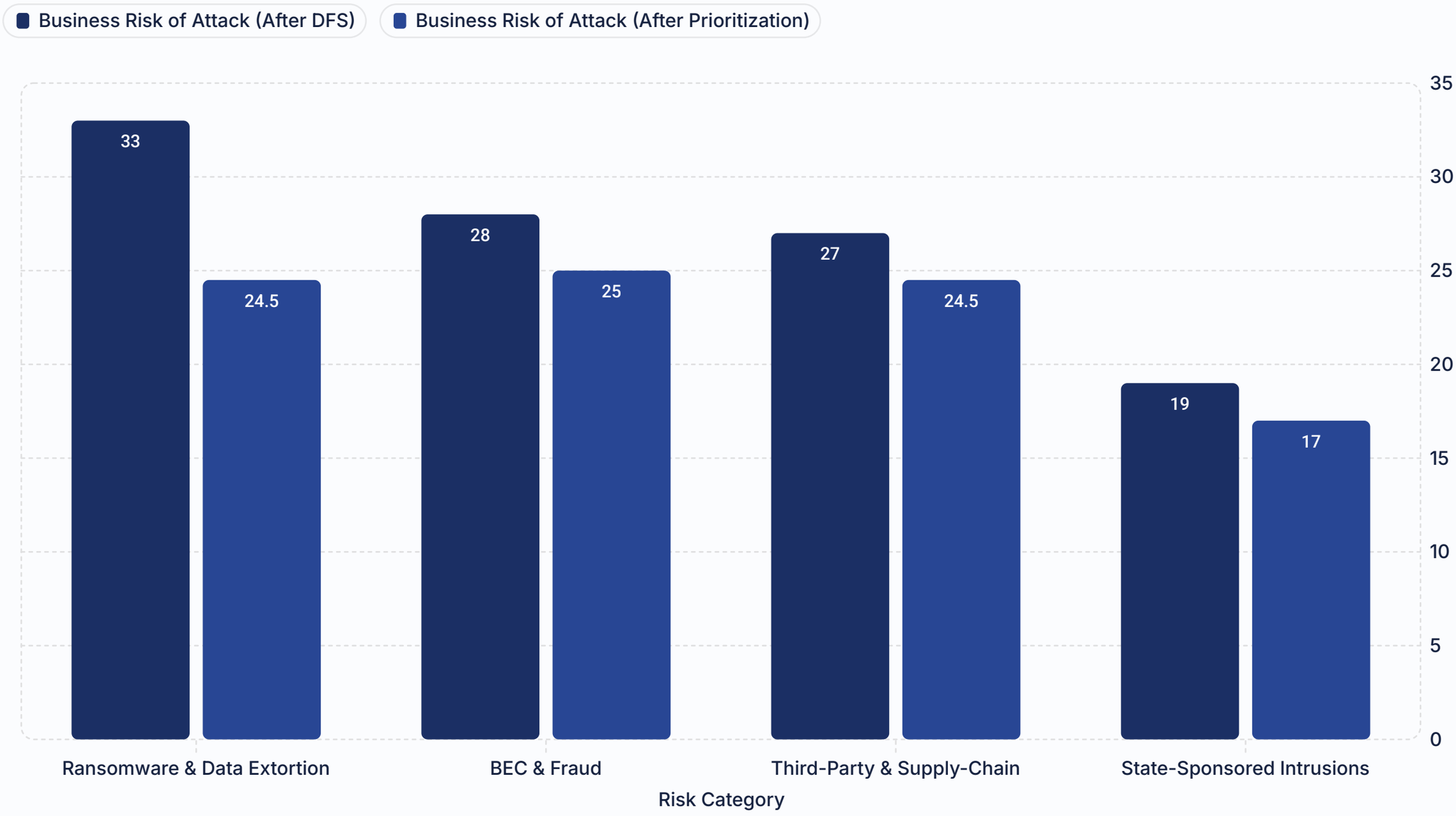
Top Risk	DFS Controls Emphasized	Prioritization Framework — Focus	Controls Elevated by Prioritization	How This Changes Outcomes	Expected Incremental Impact Beyond DFS
Ransomware & Data Extortion	Vulnerability management; SIEM/XDR; IDS/IPS; EDR; backup integrity; incident response; business continuity	**Break high-impact attack pathways** (containment, privilege, recovery failure)	**Privileged Access Management (PAM); network segmentation; EDR (containment); immutable backups; recovery validation; incident execution discipline**	Targets the specific points where ransomware becomes material (lateral movement, encryption success, failed recovery)	**High** — materially reduces probability of impact and compresses scenario likelihood by removing failure chains
Business Email Compromise (BEC) & Fraud	MFA; phishing-resistant MFA; email security; DMARC/DKIM/SPF; fraud monitoring; awareness training	**Reduce high-frequency exposure at decision points**	**Transaction verification controls; fraud workflow controls; anomaly detection; user response workflows; authentication hardening**	Interrupts attack execution at human and transactional decision stages rather than just reducing phishing volume	**Moderate** — lowers successful fraud execution rate but does not eliminate exposure due to persistent social engineering
Third-Party & Supply-Chain Attacks	Vendor risk monitoring; contractual controls; CSPM; SaaS controls; software supply chain validation	**Manage external dependency risk boundaries**	**Continuous vendor monitoring; remote access control; SaaS/CRM/ERP security controls; SBOM validation; cloud posture enforcement**	Improves detection and governance but cannot fully control external attack surfaces	**Limited** — reduces exposure conditions but does not significantly compress scenario likelihood
State-Sponsored Intrusions & Crypto Heists	Threat intelligence; SIEM/XDR; IDS/IPS; PAM; segmentation; ZTNA; CSPM	**Constrain advanced attack execution paths where possible**	**Privileged access control; segmentation; threat intelligence integration; zero trust access; monitoring depth**	Increases resistance but cannot fully disrupt sophisticated, adaptive attack paths	**Limited** — marginal reduction in impact probability; residual risk remains structurally high

Beyond DFS: How Targeted Prioritization Further Reduces Residual Risk

Top Risk	Business Resilience (After DFS)	Business Resilience (After Prioritization)	Business Risk of Attack (After DFS)	Business Risk of Attack (After Prioritization)	Expected Incremental Impact Beyond DFS	Interpretation
Ransomware & Data Extortion	~30–41%	**~20–33%** *(analytical estimate)*	~25–41%	**~15–34%** *(analytical estimate)*	**High**	The largest estimated incremental reduction appears here because the prioritization framework directly targets privileged access, segmentation, containment, encryption success, and recovery failure pathways. The DFS values are source-backed; the post-prioritization values are analytical estimates.
Business Email Compromise (BEC) & Fraud	~36–44%	**~30–41%** *(analytical estimate)*	~22–35%	**~17–33%** *(analytical estimate)*	**Moderate**	Additional workflow controls and response processes should reduce successful fraud execution, but human-process exposure remains persistent. The DFS values are source-backed; the post-prioritization values are analytical estimates.
Third-Party & Supply-Chain Attacks	~32–42%	**~28–41%** *(analytical estimate)*	~20–34%	**~16–33%** *(analytical estimate)*	**Limited**	Additional improvement is likely constrained because vendor, platform, and dependency risk remain outside direct organizational control. The DFS values are source-backed; the post-prioritization values are analytical estimates.
State-Sponsored Intrusions & Crypto Heists	~32–43%	**~28–42%** *(analytical estimate)*	~13–26%	**~9–25%** *(analytical estimate)*	**Limited**	Additional prioritization may improve resistance at the margin, but stealth, targeting, and geopolitical drivers imply residual exposure is still likely to remain meaningful. The DFS values are source-backed; the post-prioritization values are analytical estimates.

Prioritization Moves the Needle — But Residual Risk Remains

Targeted prioritization delivers incremental reduction beyond DFS — most significantly in ransomware, where discrete attack-path controls have the greatest effect on residual business risk of attack.



DFS values are source-backed. Post-prioritization values are analytical estimates based on targeted attack-path control effectiveness.

How to Prioritize in a High-Threat Environment

Prioritize the controls that change outcomes — not the ones that simply check boxes.

What Changed vs. What Didn't

What Improves	What Doesn't
Control effectiveness (ACRMI increases)	Attack likelihood remains high
Detection & response capability	Exposure to external threats
Recovery & resilience	Residual business risk

The Prioritization Problem

Not all DFS recommendations reduce risk equally.

- Some actions **directly reduce impact pathways** (high value)
- Some actions **improve resilience only** (necessary but limited)
- Some risks remain **externally driven and largely uncontrollable**

Priority Framework

Priority 1 — Break High-Impact Attack Paths

Focus where control improvements materially change outcomes:

- Ransomware containment & recovery
- Privileged access control
- Segmentation and backup integrity

Priority 2 — Reduce High-Frequency Exposure

Where likelihood stays high but impact reduction is partial:

- BEC / fraud workflow controls
- Social engineering response processes

Priority 3 — Manage External Dependency Risk

Where controls have limits:

- Third-party / supply chain risk
- State-sponsored / advanced threats

The priority framework above is not a one-time exercise — it must be revisited as threat conditions change. What reduces risk most effectively today may shift as attackers adapt and new vulnerabilities emerge.

What To Do Now

Five concrete actions executives and CISOs should take based on the findings in this report.

Assess Control Execution — Not Just Control Presence

Audit whether your top controls are being applied consistently across all environments, not just whether they are deployed. Inconsistent execution is where risk lives.

Prioritize Attack-Path Failure Points First

Concentrate investment and operational discipline on the controls that prevent attacks from becoming material events: privileged access, segmentation, containment, and recovery integrity.

Quantify Your Residual Risk

Do not assume DFS alignment means low risk. Commission or produce a quantified view of residual scenario likelihood and expected financial impact specific to your organization's profile.

Establish a Monthly Risk Forecast Cadence

Static annual assessments do not reflect how quickly the threat environment changes. Implement a monthly review of top scenario likelihood, control effectiveness, and emerging threat drivers.

Align Leadership on Residual Risk Acceptance

Bring quantified residual risk to the board and executive team. Decisions about which risks to accept, defer, or transfer require a shared, defensible view of exposure — not qualitative ratings.

The goal is not to eliminate all risk — it is to understand which risks are material, which controls change outcomes, and where residual exposure requires explicit leadership decisions.

Conclusions & Path Forward

DFS guidance is a necessary starting point — but in a heightened threat environment, it is not sufficient on its own.

What the Analysis Confirms

DFS-aligned controls materially improve business resilience — but they do not close the gap. The probability of industry-level attacks remains elevated, and residual risk stays material across all sectors and scenarios after alignment.

What Static Guidance Cannot Provide

Control checklists and sector guidance are necessary inputs, but they do not show how much risk an organization is currently carrying, how conditions are changing, or which actions will produce the greatest reduction in exposure.

The Path Forward

Organizations must move beyond static assessments and adopt continuously updated, quantified risk forecasts — ones that measure control effectiveness, track emerging threat drivers, and translate scenario likelihood into defensible business decisions.

> **The goal** is not simply to confirm that controls exist, but to **understand where risk is increasing, where recommendations will meaningfully reduce exposure, and where residual risk remains material. That is the level of analysis required to make better decisions in today's threat environment.**

About CyberRiskModels.com

Charlene Deaver-Vazquez — Cyber Risk Quantification Expert

CyberRiskModels.com delivers business-level cyber risk forecasts built on the math of probability. Founded by Charlene Deaver-Vazquez, an expert in cyber risk quantification with deep experience supporting organizations including the Nuclear Regulatory Commission, the forecasts translate complex attack patterns, threat behavior, and control effectiveness into clear, actionable business-level risk.

Risk Modeling

Scenario-based models that estimate frequency, financial impact, and control effectiveness using probabilistic techniques.

Monthly Forecasts

Business-level risk forecasts delivered monthly, tailored to your industry, exposure, attractiveness, and security maturity — for the cost of a daily latte.

> The goal is simple: to **give CISOs and business leaders a clear, defensible view of cyber risk — and the confidence to act on it.**
>
> — Charlene Deaver-Vazquez Charlene@CyberRiskModels.com