HUNTER X

PLAYBOOK

HUNTERX RISK REPORT

Account Management Playbook

Table of Contents

liongard

1. Purpose of This Playbook

This playbook is designed to help Account Management teams use the HunterX Risk Report as a recurring, high-value advisory tool for existing clients.

As an Account Manager, the goal of the Risk Report is to:

- Reinforce your role as a trusted security advisor
- Identify logical, client-aligned opportunities for service expansion
- Bring structure and data to ongoing security conversations
- Validate cyber insurance guidance and risk assumptions
- Strengthen retention and renewal conversations with objective insight

Key Principle

This playbook focuses on how Account Management teams use the **HunterX Risk Report** to strengthen relationships, align on risk over time, and guide informed security decisions throughout the client lifecycle.

2. When Account Managers Should Run the Risk Report

The HunterX Risk Report is most effective when used on a predictable, recurring cadence, not as a one-off event.

1 Recommended Cadence

- Annually for all managed clients (baseline expectation)
- Biannually for:
  - Clients in regulated or high-risk industries
  - Larger or revenue-critical accounts
  - Clients with active cyber insurance policies

Consistency matters more than frequency. Running the report on a regular cadence ensures risk conversations are grounded in current context and comparable benchmarks, rather than being treated as a one-off exercise.

2 Ideal Trigger Events

Account Managers should also run or reference the Risk Report when:

- Preparing for a QBR or vCIO session
- Supporting cyber insurance renewal discussions
- Approaching contract renewal or scope expansion
- A client experiences significant business change:
  - M&A activity
  - Growth or downsizing
  - New compliance or regulatory pressure
- A cyber incident occurs in the client’s industry

3. What the Risk Report Is

1 What the Risk Report Shows

The HunterX Risk Report provides:

- A probability-based view of cyber incident likelihood
- Industry-benchmarked comparisons against:
    - Peer organizations
    - Breached companies
    - Best-in-class security maturity
- Modeled financial impact of potential cyber incidents
- Common attack patterns and data exposure trends for the client's sector

Key Principle

This allows you to ground conversations in relative risk and business impact, rather than technical detail.

2 What the Risk Report Does *Not* Do

It is equally important to set expectations about what the report is not:

- It is not a vulnerability scan
- It does not inspect internal configurations or tools
- It does not provide step-by-step remediation instructions
- It does not guarantee that risk scores will change over time

3 How Risk Factors Should Be Interpreted

A negative risk factor does not mean an organization is insecure, negligent, or using “bad” tools.

It reflects how risk is concentrated based on externally observable patterns and how similar organizations have historically experienced cyber incidents.

In many cases, negative risk factors are influenced by factors such as:

- **Reliance on widely used platforms or services**

  Common, well-adopted technologies can represent concentrated risk because they are attractive targets and potential single points of failure.

- **Technology centralization**

  When critical business functions depend heavily on a small number of external services, the potential impact of disruption increases, even if those services are well-managed and reputable.

- **Industry-specific exposure patterns**

  Certain sectors naturally face higher baseline risk due to the type of data they handle, their operational dependencies, or how attackers typically target similar organizations.

Important clarification to share with clients:

A negative risk factor does not suggest these tools should be removed or avoided. It highlights where additional safeguards, contingency planning, or risk transfer (like insurance) may be appropriate.

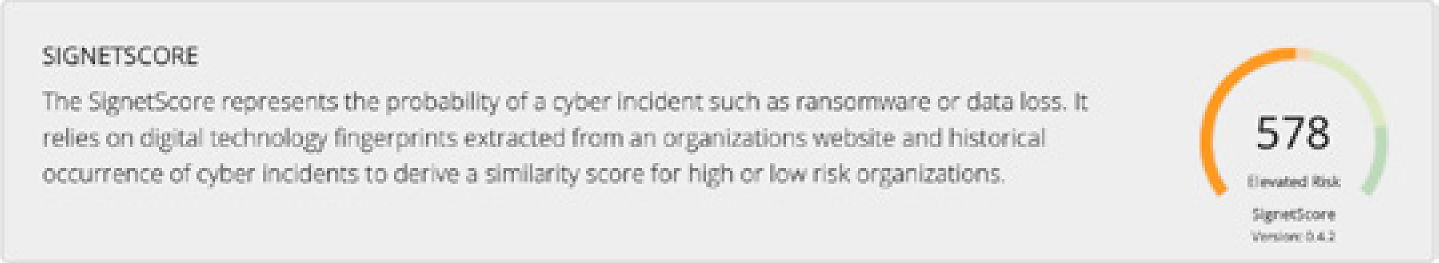
4 Recommended Client Framing

> This report gives us an external, industry-benchmarked view of cyber risk. It helps us understand how your organization compares to others like you and what that level of risk could mean for your business based on the technologies and services you rely on.
>
> A negative impact score doesn't mean something is 'wrong' or that certain tools are bad, it highlights where risk may be more centralized or impactful, so we can confirm whether your current security approach, insurance coverage, and mitigation strategy are appropriately aligned with the real-world risk organizations in your sector are facing today.

4. How Account Managers Should Read the Risk Report

The Risk Report should be interpreted holistically, not line-by-line. Account Managers are not expected to explain every chart, only to guide the conversation.

1 SignetScore



SIGNETSCORE

The SignetScore represents the probability of a cyber incident such as ransomware or data loss. It relies on digital technology fingerprints extracted from an organizations website and historical occurrence of cyber incidents to derive a similarity score for high or low risk organizations.

578

Elevated Risk

SignetScore

Version: 0.4.3

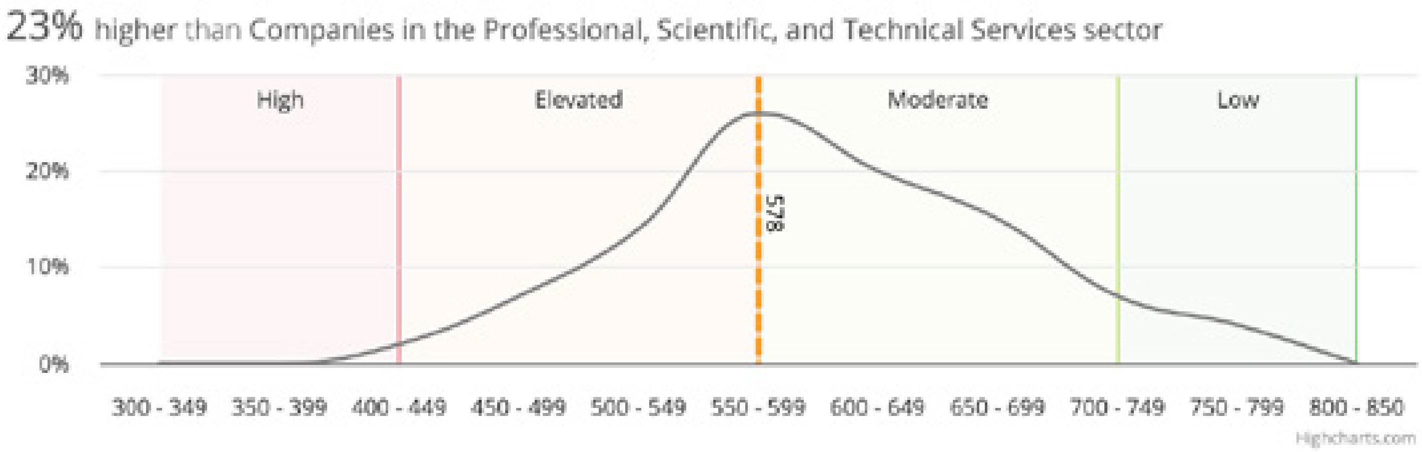
How to use it:

- Treat the score as a directional indicator, not a pass/fail grade
- Focus on relative position and trend over time
- Avoid promising score reduction

What to say:

"The score helps us understand relative risk compared to similar organizations. It's a benchmark, not a target."

2 Peer & Industry Comparisons


23% higher than Companies in the Professional, Scientific, and Technical Services sector

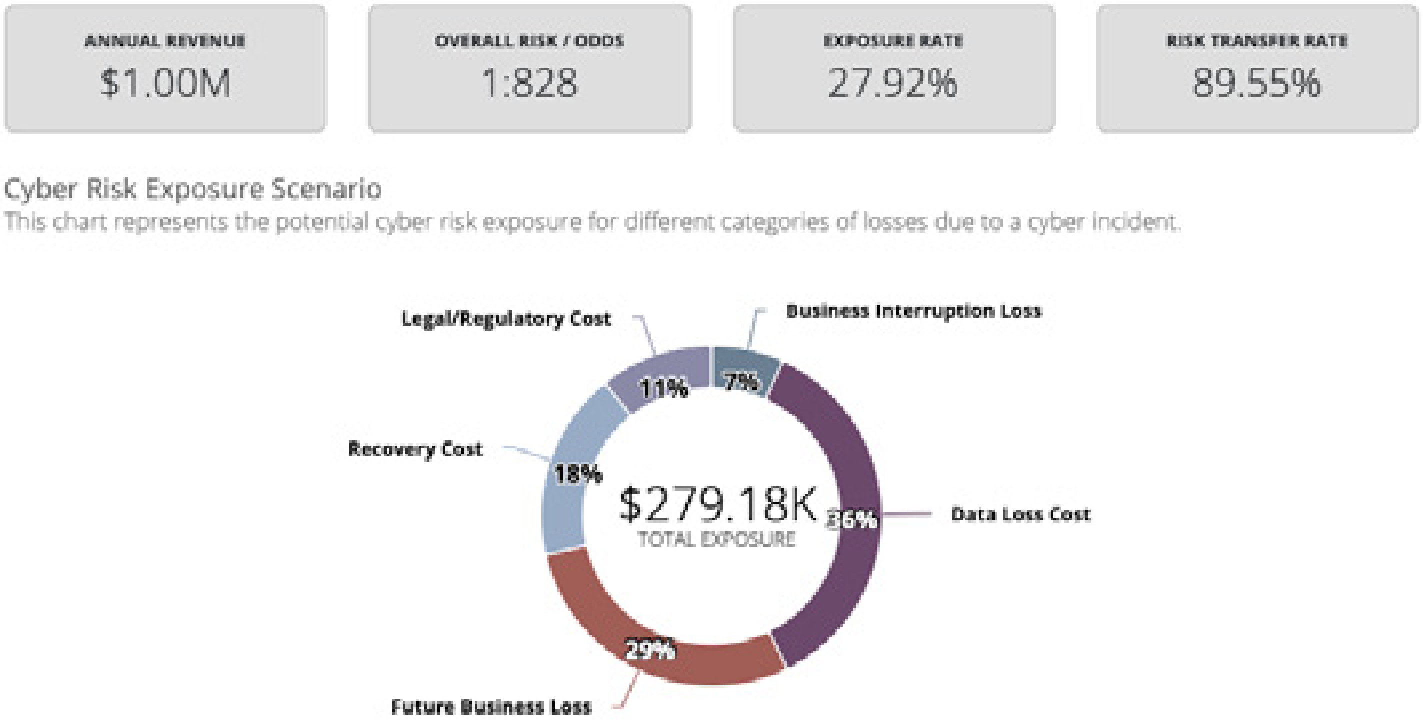
How to use it:

- Anchor discussions in context, not alarm
- Highlight gaps or strengths compared to peers

Why it matters:

- Clients respond better to comparisons than absolutes
- This grounds security conversations in objective, real-world context rather than isolated data points.

3 Cyber Risk Quantification



ANNUAL REVENUE
$1.00M

OVERALL RISK / ODDS
1:828

EXPOSURE RATE
27.92%

RISK TRANSFER RATE
89.55%

Cyber Risk Exposure Scenario

This chart represents the potential cyber risk exposure for different categories of losses due to a cyber incident.

How to use it:

- Translate cyber risk into business language
- Use modeled exposure to support prioritization and planning

What to emphasize:

- These are probability-weighted scenarios, not predictions
- The purpose is decision support, not fear

Note: Insurance inputs in this section are automatically populated using industry-average assumptions. When a client's actual cyber insurance limits or coverage details are available, Account Managers may update these values to better reflect the client's real risk transfer posture.

[Learn how to update insurance inputs]

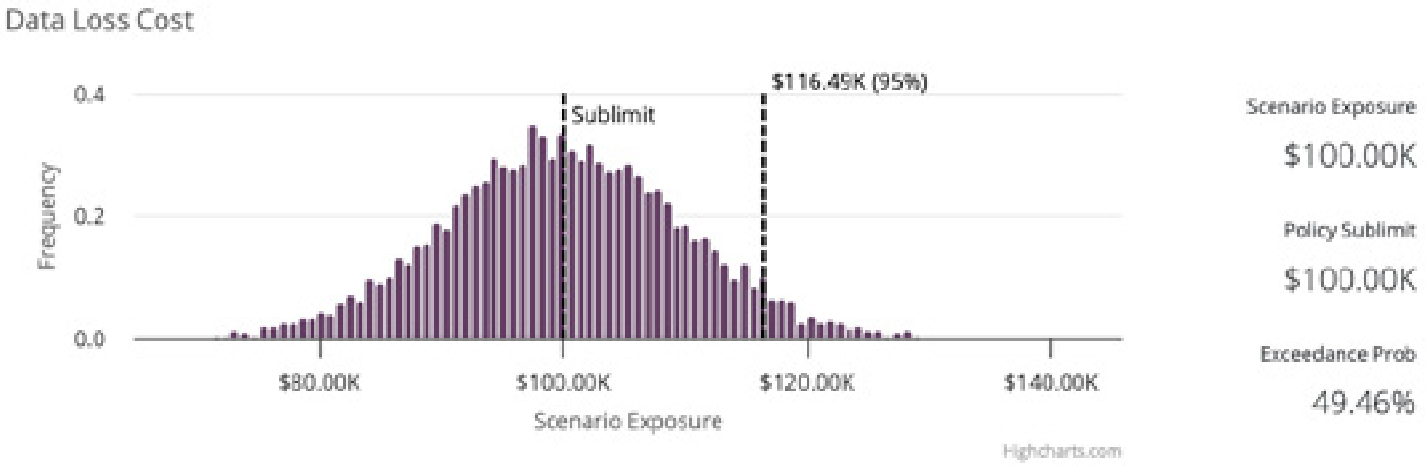
4 Insurance Coverage & Residual Risk

How to use it:

- Validate whether current insurance coverage aligns with modeled exposure
- Identify residual risk that may remain even with coverage

Why this is powerful:

- Supports insurance conversations with objective data
- Protects your organization by documenting advisory guidance

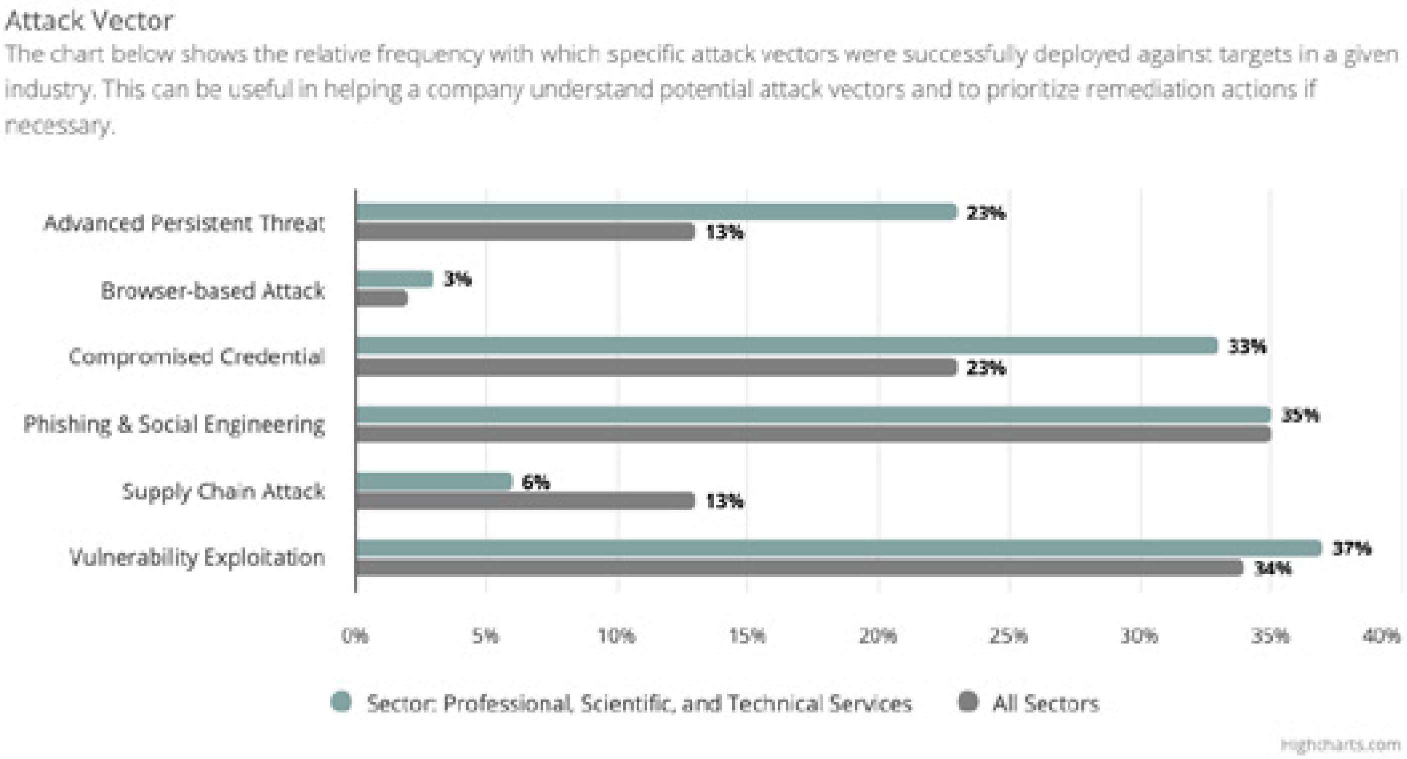


Scenario Exposure
$100.00K

Policy Sublimit
$100.00K

Exceedance Prob
49.46%

5 Industry Attack & Data Trends



Attack Vector

The chart below shows the relative frequency with which specific attack vectors were successfully deployed against targets in a given industry. This can be useful in helping a company understand potential attack vectors and to prioritize remediation actions if necessary.

How to use it:

- Normalize the conversation ("this is common in your sector")
- Help clients understand where attackers typically succeed
- Identifies areas to potentially strengthen within the business

Note for AMs: This section helps identify where additional services or controls may be appropriate based on common attack patterns. This can be used to guide prioritization and alignment conversations

5. Using the Risk Report in QBRs & vCIO Conversations

The HunterX Risk Report is most effective when embedded into existing account management rhythms, not introduced as a standalone security exercise.

For most, this means positioning the report within:

- Annual or biannual QBRs
- vCIO strategy and roadmap discussions
- Renewal-adjacent planning meetings

1 Where the Report Fits in a QBR

Recommended placement:

- Right before future-state planning

This sequencing matters. It ensures the risk conversation:

- Builds on established trust
- Feels contextual, not reactive
- Naturally feeds into roadmap and prioritization

2 Recommended Conversation Flow

Account Managers should guide the discussion in this order:

1. Current Position

> “Here’s how your external cyber risk profile looks today, relative to your peers.”

2. Industry Context

> “Here’s what organizations like yours typically experience when incidents occur.”

3. Business Impact

> “Here’s what that risk could realistically mean in financial and operational terms.”

4. Planning & Alignment

> “Based on this, let’s talk about whether our current strategy and coverage still make sense.”

The goal is alignment **vs.** agreement on every control or service.

3 What Success Looks Like in a QBR

- The client feels informed, not alarmed
- Service value is clearly tied to business impact and risk alignment.
- Risk ownership is shared, not shifted entirely to your organization
- Security discussions move from reactive to planned
- Follow-up actions feel logical, not forced

6. Validating Cyber Insurance Recommendations

Cyber insurance is one of the most common, and most sensitive, topics Account Managers navigate. The Risk Report provides an objective foundation for these conversations.

1 How Account Managers Should Use the Report

The Risk Report helps AMs:

- Compare modeled financial exposure against current policy limits
- Identify residual risk that remains after insurance
- Validate whether coverage assumptions are still reasonable as the business evolves

This is not about replacing brokers or policies. It is about sanity-checking risk alignment.

2 Recommended AM Framing

> “This report helps us sanity-check whether your current cyber insurance coverage still aligns with what organizations like yours typically experience. It gives us an objective way to support those conversations as your business and risk profile evolve.”

3 Common Scenarios Where This Adds Value

- Policy renewals or broker reviews
- Rapid company growth without updated coverage
- Industry-wide ransomware awareness

4 Outcomes for the Your Organization

- Stronger documentation of advisory guidance
- Reduced liability through data-backed recommendations
- Increased client confidence in security planning

7. Identifying Upsell & Expansion Opportunities

The Risk Report supports expansion when used as a risk-alignment tool, not a sales trigger.

1 Expansion Signals to Watch For

Account Managers should look for:

- High modeled financial exposure relative to revenue
- Meaningful gaps compared to peer benchmarks
- Elevated ransomware payment likelihood
- Significant residual risk after insurance

These signals indicate misalignment, not failure.

2 Mapping Risk Signals to Services

Use the report to guide *which* conversations to have, not *what to sell.*

Common alignments include:

- Security posture or maturity reviews
- Backup and disaster recovery validation
- Email and identity security enhancements
- Security awareness and training programs
- Incident response planning and tabletop exercises

3 AM Guardrails

- Do not lead with tools or SKUs
- Do not promise risk score reduction
- Do not frame services as urgent fixes unless there is an active incident

4 Example AM Language

> "Based on what we're seeing industry-wide, there may be an opportunity to better align your current services with your risk profile. Let's talk through options and priorities together."

8. Client Communication Templates

Account Managers should set expectations clearly before sharing or discussing the Risk Report.

1 Pre-QBR / Pre-Review Email (Purpose Setting)

Key Elements to Include:

- Why the report is being run
- What the report will and will not show
- How it will be used in the conversation

Example framing:

> “Ahead of our upcoming review, we’ll be sharing an industry-benchmarked cyber risk report. This helps us ground our discussion in how organizations like yours are typically impacted and whether our current strategy still aligns.”

Subject: Preparing for our upcoming review

Hi {{First Name}},

As part of our upcoming review, we’ll be sharing an industry-benchmarked cyber risk report that provides an external view of how organizations like yours typically compare across your sector.

This report helps us ground our discussion in relative risk and potential business impact, not internal configurations or one-off findings. It’s designed to support planning and alignment as your business evolves.

We’ll walk through the highlights together during our meeting and discuss whether our current approach still makes sense.

Looking forward to the conversation,

[Signature]

2 Post-QBR Follow-Up (Documentation & Alignment)

Key Elements to Include:

- Summary of key takeaways
- Areas of alignment and open questions
- Any agreed next steps or follow-ups

Example framing:

> “Based on our discussion, we’ll continue monitoring your risk profile annually and revisit coverage and service alignment as the business evolves.”

These communications reinforce your organization’s advisory role and create a paper trail of guidance.

Subject: Summary from our recent review

Hi {{First Name}},

Thanks again for taking the time to walk through the cyber risk report together.

As discussed, the report helps provide context around how organizations like yours typically experience cyber risk and the potential business impact associated with those scenarios. It was helpful in validating where your current strategy is aligned and where we may want to continue monitoring over time.

We’ll plan to revisit this annually as part of our regular review cadence and adjust recommendations as the business or risk landscape changes.

Please let me know if you’d like to go deeper on any of the areas we discussed.

Best,

[Signature]

3 Cyber Insurance Review Email (Alignment & Validation)

Cyber Insurance Review Email (Purpose Setting)

Key Elements to Include:

- Why the report is being referenced
- What the report will and will not do
- How it supports insurance conversations (without replacing brokers)

Example framing:

> “We use this report to help validate whether coverage assumptions still align with how organizations like yours are typically impacted, not to recommend specific policy changes.”

Subject: Supporting your upcoming cyber insurance review

Hi {{First Name}},

Ahead of your upcoming cyber insurance review, we wanted to share an industry-benchmarked cyber risk report that we run as part of our standard advisory process.

This report provides an external, probability-based view of cyber risk and potential business impact for organizations like yours. It’s not an assessment of internal configurations, and it’s not a recommendation to change coverage. It’s simply a way to help validate whether current assumptions still align with today’s risk landscape.

If helpful, we can walk through the highlights together and discuss how this may support your conversation with your broker.

Best,

[Signature]

4 Risk Alignment / Expansion Email

Risk Alignment Follow-Up Email (Purpose Setting)

Key Elements to Include:

- Why the report is being referenced now
- Clear reassurance that nothing is “wrong” or urgent
- How it supports planning and prioritization over time

Example framing:

> “This isn’t about immediate action, it’s about ensuring services and strategy continue to align as risk and the business evolve.”

Subject: Aligning services with your current risk profile

Hi {{First Name}},

As part of our recent risk review, we identified a few areas where organizations in your industry are typically reassessing priorities as their risk profile and operations evolve.

This doesn’t indicate that anything is wrong or requires immediate action. The report is designed to support longer-term planning and help ensure that services and coverage continue to align with where the business is today and where it’s headed.

If it’s useful, we’re happy to walk through those areas together and discuss whether any adjustments are worth considering over time.

Best,

[Signature]

9. Common Pitfalls & What to Avoid

To preserve trust and credibility, **Account Managers should avoid the following:**

- Treating the Risk Report like a vulnerability or compliance audit
- Over-indexing on the numerical score
- Promising that actions will reduce the score
- Using fear-based language or urgency
- Jumping directly to tools, SKUs, or packages

Reminder:

The Risk Report is designed to inform decisions, not force outcomes.

10. Measuring Success

To understand the impact of the Risk Report within Account Management, you should track:

- Percentage of accounts with an annual or biannual Risk Report cadence
- QBRs or vCIO meetings where the report is referenced
- Insurance renewal discussions supported by the report
- Expansion conversations influenced by risk alignment
- Retention and renewal outcomes

These metrics help validate the report as a relationship and retention asset, not just a sales tool.

11. Account Manager Checklist

To understand the impact of the Risk Report within Account Management, you should track:

1 Before the meeting

- ### Confirm timing & purpose

  □ Is this an annual or biannual review?

  □ Is this tied to a QBR, renewal, or insurance review?

- ### Prepare the narrative

  □ I know why we're reviewing the Risk Report now

  □ I can explain what the report will and will not show

  □ I've sent (or plan to send) the pre-review email

- ### Quick scan of the report

  □ Reviewed SignetScore and risk tier (for context only)

  □ Noted peer and industry comparisons

  □ Identified key financial exposure ranges

  □ Checked insurance coverage and residual risk sections

2 During the Conversation

- ### Set expectations early

  □ Clarified this is an external, benchmarked view

  □ Reinforced that this is not an internal audit or scan

- ### Guide the discussion (don't deep dive)

  □ Anchored risk in peer and industry context

  □ Used financial impact to translate technical risk

  □ Normalized risk using industry trends

  □ Kept the focus on alignment, not urgency

- **Watch for alignment signals**
  - □ Client asked about insurance coverage
  - □ Client referenced business impact or downtime
  - □ Client connected risk to future planning

3 After the Meeting

- **Document and reinforce**
  - □ Sent post-QBR follow-up summary
  - □ Documented areas of alignment and open questions
  - □ Confirmed next review cadence (annual / biannual)
- **Optional follow-ups**
  - □ Insurance alignment discussion (if relevant)
  - □ Planning or prioritization conversation
  - □ Review of services vs evolving risk profile

4 What to Avoid

- □ Don’t sell tools or SKUs
- □ Don’t promise risk score changes
- □ Don’t create urgency unless there’s an active incident
- □ Don’t use fear-based language
- □ Don’t treat this like a vulnerability report

Final Reminder

The HunterX Risk Report is a planning and alignment tool. When used consistently, it builds trust, supports better decisions, and reinforces your role as a long-term security advisor.

Ready to take a more aggressive stance on sales and security?

Activate HunterX.
Take the attack surface by storm

About Liongard

Liongard is redefining asset intelligence with its AI-powered platform built for modern IT and security operations. Trusted by organizations worldwide to protect complex environments, Liongard delivers unified, real-time visibility across users, systems, networks, and SaaS Applications. Liongard empowers teams to uncover hidden risks, enforce controls, and automate critical security outcomes. By combining deep asset intelligence with AI-driven insights and scalable remediation, Liongard helps organizations reduce risk, strengthen cyber resilience, and operate more efficiently.

For more information, visit www.liongard.com

liongard