Messaging, Malware, and Mobile Anti-Abuse Working Group

M³AAWG Building a Business Case for an Abuse Desk

Published November 2026
The reference URL for this document is m3aawg.org/AbuseDeskBusinessCase

Table of Contents

Introduction: Making the Business Case for an Abuse Desk 1

Understanding the Business Case Format 3

Framing the Problem for Executives 5

Calculating the Costs and ROI of an Abuse Desk 7

Operational and Staffing Considerations 11

Presenting Your Business Case 13

Conclusion 14

References 14

Introduction: Making the Business Case for an Abuse Desk

The Abuse Desk is often treated as a reactive function—funded just enough to contain major incidents but not equipped to prevent them. Executives often see abuse management as a cost center, something to minimize rather than invest in. As a result, Abuse Desks are frequently understaffed, underfunded, and unable to keep pace with evolving threats.

Confounding the problem are the numerous flavors and labels given to an abuse desk, including Trust & Safety, Platform Integrity, Customer Protection, Incident Management, Compliance Team, and more. The proliferation of terms and labels creates another layer of complication when discussing strategy and funding for the role. Many abuse organizations struggle to demonstrate impact because the underlying telemetry, categorization, attribution, and cost data were never designed to measure abuse outcomes.

Yet the consequences of under-resourced abuse handling reach far beyond day-to-day operations, affecting revenue, customer trust, regulatory exposure, and overall business resilience. The scale of the challenge is global:

- An estimated **3.4 billion** phishing emails are sent daily, representing one of the most prevalent cyber threat vectors.[1]

- **3.8 million** phishing attacks were recorded globally in 2025, reflecting sustained high-volume targeting across sectors. [2]
- Approximately **45%** of global email traffic is classified as spam or potentially harmful.[3]
- **94%** of businesses report phishing attempts within a given year. [4]

At the current scale, abuse is not episodic but systemic, with billions of malicious emails, SMS, phone calls, domains purpose-built for fraud, account takeovers, and more, sent and created daily, with nearly every organization being regularly targeted. Despite these risks, securing funding for an Abuse Desk can be challenging. Executive leadership often prioritizes revenue-generating initiatives, making it difficult for Abuse Desk managers to justify operational investments.

Because the costs of neglecting abuse handling are high, a well-structured business case becomes essential. Here are just some examples of the losses associated with abuse:

- Revenue loss from email deliverability issues, blocklisted IPs, and account abuse.
- Reputational damage when platforms fail to prevent phishing, spam, or fraud.
- Legal and regulatory risks (fines and litigation costs) due to non-compliance with the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Canada's Anti-Spam Legislation (CASL), and other laws.

This document will help email service providers (ESPs), mailbox providers (MBPs), internet service providers (ISPs), hosting companies, and other technology companies in similar situations build a persuasive business case for an Abuse Desk. For this document, "Abuse Desk" refers to a function responsible for receiving, analyzing, and mitigating reports of abuse across messaging, hosting, or network infrastructure, including spam/phishing/malware, device intrusion, account takeover, fraud, and policy violations.

Not everyone will be starting from scratch. Many organizations already have an abuse function, either as a dedicated team under budget review or as a part-time role within Support, Operations, or Security. The main goal is often to defend or expand this function, rather than build it from the ground up. Defending an existing team can be tough because effective work makes abuse less visible and the impact may not be calculable, which sometimes leads to budget cuts. To avoid this, set clear metrics and key performance indicators (KPIs) to show ongoing value from the start and report on them regularly. Use the cost-of-inaction formulas in this document to highlight what the team currently prevents, and frame any proposed cuts as a choice to move those risks and costs back onto the balance sheet.

The guidance provided here is intended to be adaptable and scalable. Metrics, staffing models, and tooling will vary by organization size, industry, and region. The document addresses the following functions:

- Identify the core components of a strong business case, including cost analysis, ROI projections, and operational requirements.
- Frame abuse management as a business-critical function rather than a cost center.
- Address common executive objections and build a compelling investment case.
- Present your business case clearly and persuasively to decision-makers.

By the end of this guide, you will have the structure, language, and supporting points needed to secure executive buy-in and help ensure your Abuse Desk has the resources needed to protect both your organization and its customers.

Understanding the Business Case Format

A well-structured business case is the key to securing executive buy-in for an Abuse Desk. While abuse management teams understand the critical role they play, executives need a clear, data-driven, and compelling proposal that aligns with business priorities. The goal is to present the Abuse Desk as an essential investment, one that supports business objectives, reduces risk, protects revenue, and ensures regulatory compliance.

A strong business case typically includes the following components:

1. Executive Summary

A concise, high-level overview that outlines:

- The problem (e.g., rising abuse cases, increasing compliance risks, revenue loss due to deliverability issues, legal risks, and, in extreme cases, scrutiny from law enforcement).
- The proposed solution (establishing or expanding the Abuse Desk).
- The expected benefits (cost savings, risk reduction, operational efficiency, customer satisfaction).

This section should be brief but impactful, setting the stage for the following details.

2. Problem Statement: Why Action Is Needed Now

Executives are more likely to approve funding when they clearly understand the consequences of inaction. This section should:

- Define and detail the current abuse challenges (e.g., elevated phishing attacks, spam complaints, block listings, account takeovers, etc.).
- Quantify the impact (financial losses, customer churn, regulatory risks, social backlash).
- Provide relevant data, such as increasing abuse reports, declining sender reputation, or legal warnings from regulators, law enforcement, and trusted industry actors.

A compelling problem statement frames abuse management as a business-critical issue rather than a secondary operational concern.

3. Cost Analysis and Return on Investment: The Financial Case

One of the most effective ways to justify an Abuse Desk is by demonstrating its financial impact. This section should outline:

- Current costs of inaction, including lost revenue due to blocked emails, customer churn, lost leads, time spent handling escalations, or fines for non-compliance.
- Projected costs of the Abuse Desk, including staffing, software, and training.
- Return on Investment (ROI) by showing how proactive abuse management reduces costs (e.g., fewer compliance fines, improved deliverability, reduced customer support burden, more renewals).

Data-driven projections will strengthen your argument. If available, use case studies or industry benchmarks to frame your argument. To the extent that you can base your argument on internally sourced data, you will be better positioned to demonstrate the costs of insufficient investment in the abuse desk.

4. Operational Requirements: What's Needed to Succeed

Decision makers want to have a clear understanding of what it takes to build and sustain an effective Abuse Desk. This section should outline:

- Staffing needs (number of analysts, specialized roles, consultants).
- Technology and tooling (abuse report automation, fraud detection systems, AI modeling, reputation monitoring tools, observability tools across the customer lifecycle to find weaknesses and leaks in the funnel as a result of abuse).
- Processes and workflows for handling abuse reports, investigations, and escalations. This should include not just Abuse Desk processes, but also the alignment of processes between the Abuse Desk and the rest of the organization (especially Business/Sales and Product/Engineering).

This section should balance realistic budget considerations with critical needs.

5. Risk Assessment: What Happens if We Don't Act?

Every executive wants to minimize risk, and this section helps reinforce why funding the Abuse Desk is a strategic priority. It should cover:

- Reputational damage, including customer trust issues, negative media, and public relations crises.
- Operational risks, like being blocked by major mailbox providers, third-party blocklisting, or increased fraud on your platform.
- Legal risks, such as compliance violations, GDPR fines, or FTC investigations.

You may want to consider creating a tiered model that defines good, better, and best approaches. Executives must balance and justify heavy investment in personnel and technology with free cash flow, R&D, development, and growth costs of other parts of the business. Creating a plan that links improvements to investment at three levels—what will happen with no investment, minimal investment, or fully funding the project—gives you a fallback if executives balk at the fully funded model. Remember, your executive team is responsible for every dollar spent at your company. Although your request is important, every team's request for funding is also important, and making optimal financial decisions will help to ensure the success of the entire organization. The more context and structure you can put into your proposal, the more likely it is to be taken seriously.

There is often a strong case for expanding the abuse function. When abuse work is spread across different teams as a temporary solution, the Full-Time Employee (FTE) opportunity cost formula (covered in "Calculating the Costs and ROI of an Abuse Desk" below) shows the real costs: how much are Engineering, Support, and Legal spending on this work now, and what important tasks are they missing as a result? Organizations that already have processes and ownership in place with borrowed staff are in a good position to use this tiered model. The lowest tier is usually the current, stretched, and decentralized model. This changes the request from asking leaders to trust a new idea to asking them to fund roles for a model that already works, which makes executive approval more likely.

6. Conclusion and Recommendation

This section ties everything together with a clear ask:

- A summary of the problem and proposed solutions.
- A direct funding request with cost breakdowns and assumptions based on tiered funding approaches.
- A timeline of next steps with milestones detailing implementation and when mitigation can be expected.
- A call to action for executive approval.

Framing the Problem for Executives

Building a strong business case for an Abuse Desk isn't just about explaining the problem; it's about presenting it in a way that resonates with decision-makers. Executives have different priorities, and their buy-in depends on how well you can frame the Abuse Desk's value in terms they care about.

1. Identify Your Key Stakeholders

Before making your case, understand who in the company will influence the decision. For example:

- **Finance**: Focuses on cost savings, allocating funding for additional headcount, revenue protection, and long-term ROI.
- **Product**: The product is the heart of the matter. If abuse is to be stopped in a meaningful way, then you may need to advocate for changes to product features, onboarding flows, and the user lifecycle. Partnering with the product will help you decide where changes may need to happen, understand the existing roadmap, and how your changes could affect that. Conversely, it's important to position the Abuse Desk as a partner to the product team, assisting with pre-launch abuse/threat modeling, required telemetry, mitigation hooks, enforcement considerations, and post-launch monitoring.
- **Legal & Compliance**: This is concerned with regulatory risks, liability, and brand protection.
- **Engineering & Operations:** These are your technical partners, who will have a hand in implementing any new tools or changes to your technology where abuse might be happening.
- **Customer Success & Support**: This is the front line that feels the pain by fielding angry customer complaints; they're focused on preventing customer churn and mitigating negative feedback.
- **Security (CISO / VP of Security):** In organizations where the Abuse Desk reports into or alongside the security function, the CISO or VP of Security may be a key budget holder or sponsor. Their concerns center on threat surface reduction, incident response metrics, threat intelligence sharing, and alignment with the broader security operations posture. Frame the Abuse Desk as an extension of the security mission—not a separate silo—and emphasize how abuse telemetry enriches threat intelligence.

Each of these groups has different concerns, so tailor the messaging accordingly (taking care to ensure the overall message is fully consistent across groups). Oftentimes, multiple modified presentations might be needed. Build on and incorporate each stakeholder's feedback for the final presentation to the executive team, who will ask questions that run the gamut of how this investment will affect other parts of the business.

2. Customize Your Pitch for Different Executives

To make your case persuasive, align your arguments with what matters most to each stakeholder:

- **For Finance**
    - Show the fiscal impact of increased contacts or customer churn due to deliverability or security issues.
    - Highlight potential cost savings from reducing engineering and support overhead.
    - Present ROI estimates (covered in "Calculating the Costs and ROI of an Abuse Desk").
    - Understand the ramifications and be prepared to hire more personnel in geographies that are more competitive in terms of salary than North America.
- **For Product**
    - Detail how mitigating abuse will improve the customer funnel.
    - Highlight how abuse mitigation can improve roadmap velocity for engineering and product work in times of crisis by linking abuse mitigation to efficiency.
    - Understand how new features can impact the work of the Abuse Desk and highlight that an Abuse Desk can provide a sounding board for product managers to use when pressure-testing new products and features.
- **For Legal & Compliance**
    - Emphasize regulatory risks (GDPR, CAN-SPAM, CASL), potential fines, and class action litigation.
    - Show how proactive abuse mitigation prevents lawsuits and compliance violations.
    - Position the Abuse Desk as a risk-reduction investment.
    - Understand your existing Acceptable Use Policies (AUPs) and Terms of Service (ToS), as you may want to lobby for changes to these core documents based on the future actions of the Abuse Desk.
- **For Engineering & Operations**
    - Demonstrate how abuse issues create unnecessary work for engineers.
    - Explain how an Abuse Desk can streamline processes, reducing engineering burden.
    - Showcase AI, automation, or tooling improvements that free up resources.
- **For Customer Success & Support**
    - Highlight how abuse-related issues lead to customer frustration and churn.
    - Show that a proactive Abuse Desk can reduce support tickets and escalations.

    - Emphasize how a safer, more reliable platform improves customer retention.
- **For Security**
    - Highlight how an expanded Abuse Desk will decrease the burden on security personnel often charged with assisting the Abuse Desk or picking up the slack.
    - Detail how the Abuse Desk will hand over only the most severe or sensitive issues to security for handling, while expanding ownership of lower priority issues.
    - Develop a position on how Abuse Desk tooling can surface security issues through front-line intelligence and awareness, and how that data is surfaced to the security team.

3. Anticipate and Overcome Common Pushbacks

Even with a well-structured and aligned business case, you may encounter skepticism from executives who may not understand the industry, fully grasp the scope of abuse-related issues, or understand the necessity of having a well-staffed team. To strengthen your case, be prepared to address these objections with clear data and real-world examples.

The following are common objections you may hear when acting as a champion for an Abuse Desk:

- **"Can't our existing teams manage this?"** Some may believe that abuse-related issues can be absorbed by Support, Engineering, or Compliance teams without requiring a dedicated function.
- **"Is abuse really that big a problem?"** If your company hasn't yet faced a major incident, leadership may underestimate the financial and operational impact.
- **"How do we know this will be worth the cost?"** Decision-makers often want hard numbers proving the ROI before committing resources.
- **"Won't this create unnecessary friction for customers?"** Certain stakeholders may worry that stronger enforcement mechanisms will lead to more customer complaints or cancellations.
- **"Can't we just automate abuse detection?"** While automation can help, executives may overestimate its effectiveness and undervalue the need for human oversight in nuanced abuse cases.
- **"We already have a SOC/security team — why do we need a separate Abuse Desk?"** This is a common objection in organizations where abuse functions are consolidated under security operations. The key counterargument is that abuse handling addresses a distinct set of actors, behaviors, and stakeholders (e.g., customers, partners, and ISPs) that fall outside the typical threat-actor focus of a SOC. An Abuse Desk complements the SOC by overseeing high-volume, policy-driven cases that would otherwise consume scarce SOC analyst capacity.
- **"Our vendors manage this."** Many organizations assume that their email filtering provider, cloud hosting vendor, or security platform makes a dedicated Abuse Desk unnecessary. In practice, vendors handle abuse at a platform level but cannot act on organization-specific policy, customer relationships, or regulatory obligations. Additionally, vendors only handle abuse on their products or platforms; thus, they're unable to tackle the problem at a holistic level. An internal Abuse Desk provides contextual judgment, accountability, and an escalation path that no third-party vendor can replicate.

Calculating the Costs and ROI of an Abuse Desk

Executives don't approve budgets based on assumptions; they need real numbers to justify the investment. To make a compelling case, it's critical to quantify both the **cost of inaction** and the **return on investment** (ROI) of an Abuse Desk. Below are a few examples and calculations that might be helpful. When compiling and creating metrics and projections to detail how action or inaction may affect the handling of abuse, it is beneficial to use a tiered system of low/base/high to provide a range of projections vs. a single value.

The Cost of Inaction

1. Customer Churn Due to Reputation Issues

When a service provider gains a reputation for allowing abuse, whether through spam, phishing, or malicious hosting, it can lead to degraded performance or unmet customer expectations. As a result, legitimate customers may leave in search of more reliable alternatives. One way to quantify this impact is:

(Churn Rate % Due to Abuse × Total Customers) × Avg. Revenue per Customer = Cost of Churn.

Example:

- Churn Rate Due to Abuse: **5% (0.05)** – meaning 5% of customers leave due to abuse-related issues.
- Total Customers: **10,000** – total number of paying customers.
- Avg. Revenue per Customer: **$500** per year – the average annual revenue from each customer.

(0.05 x 10,000) x 500 = **$250,000 per year**

This simple calculation can and should be performed on different cohorts of customers to understand how it affects customer lifecycle and lifetime value. Start with recent cohorts of 30, 60, and 90 days and expand the model to longer, more established customers. Do the same exercise by grouping across revenue. Are you seeing more customer churn at the low end, or are you seeing customer churn in a revenue cohort of some of your most important customers? The latter group is the hardest and most expensive customer from an acquisition and retention standpoint.

2. Support and Compliance Costs from Abuse-Related Contacts

Abuse often generates high volumes of support tickets, compliance escalations, and legal inquiries, increasing operational costs. In all likelihood, this formula will need to be broken down by role (support, compliance, legal), but a typical support cost formula might look like:

(Abuse Tickets per Month × Avg. Handling Time) × Support Hourly Rate = Support Cost

Example:

- Abuse Tickets per Month: **200** – number of support cases related to abuse (e.g., block listings, spam complaints, phishing takedowns).
- Avg. Handling Time: **30 minutes (0.5 hours)** – average time a support/compliance agent spends resolving an abuse-related ticket.
- Support Hourly Rate: **$40 per hour** – fully loaded cost per support agent (including salary, benefits, and overhead).

(200 × 0.5) × 40= **$4,000 per month**

3. Infrastructure and Network Resource Drain

Abusive senders and bad actors may consume excessive system resources, driving up costs for maintaining IPs, servers, and bandwidth. While getting into these calculations may be a bit tricky, a basic example might be:

(% of Traffic Attributable to Abuse × Total Hosting/Network Costs) = Abuse Infrastructure Cost

Example:

- % of Traffic Attributable to Abuse: **15% (0.15)** – an estimate of the system capacity (email volume, bandwidth, or server processing) that is consumed by abusive users.
- Total Hosting/Network Costs: **$500,000 per year** – the company's total infrastructure costs for maintaining email servers, IP addresses, bandwidth, and storage.

(0.15 × 500,000) = **$75,000 per year**.

4. Brand and Reputation Damage Cost

Reputational damage from a high-profile abuse incident is one of the most compelling cost categories for a C-suite audience, yet it can be difficult to quantify. A basic approach ties estimated negative media exposure to a cost-per-impression equivalent:

(Estimated Negative Media Impressions from Incident × Cost per Impression Equivalent) + (Estimated Customer Acquisition Cost × Projected Customer Loss) = Brand Damage Cost

Your marketing or communications team may be able to help benchmark a cost-per-impression figure from past campaigns. Even a rough estimate grounds this cost category in a number, which is far more persuasive than a qualitative statement about "reputational harm."

5. Email Deliverability Revenue Loss

For ESPs and ISPs, blocklisting directly translates to lost revenue as legitimate customers cannot reach their recipients, leading to customer churn and lost revenue. This formula makes the impact concrete:

(% of Email Volume Blocked During Blocklisting Event × Total Monthly Email Volume) × Average Revenue per Delivered Message = Deliverability Revenue Loss

6. FTE Opportunity Cost

Without a dedicated Abuse Desk, abuse-related work absorbs time from engineers, legal staff, and support agents who have other primary responsibilities. This cost is often invisible in the budget but real in its drag on productivity. Quantifying it reframes the Abuse Desk as a productivity investment, not merely a cost:

(Hours Spent per Month on Abuse Tasks by Non-Abuse Staff × Fully Loaded Hourly Rate per Role) = FTE Opportunity Cost

Apply this calculation separately for each affected team (Engineering, Legal, Support) and tally the results. The total often surprises leadership and provides a compelling argument that a dedicated Abuse Desk pays for itself in recaptured productivity alone.

Additional Cost-of-Inaction Formulas

Organizations vary in size, priorities, and operating models. Depending on your environment, the following formulas may also be useful when estimating the cost of inaction:

Incident Response and Escalation Costs

(Incident Volume per Month × Avg. Time to Investigate) × Hourly Rate of Response Team = Incident Response Cost

Customer Support Overhead Due to Blocklistings

(Blocklist-Related Tickets per Month × Avg. Handle Time) × Support Hourly Rate = Blocklist Support Cost

Account Takeover (ATO) and Fraudulent Activity Losses

(Fraudulent Accounts per Month × Avg. Loss per Incident) + Chargeback Fees = Fraud Loss Cost

Regulatory and Legal Risk Exposure

(Fine per Violation × Estimated Violations per Year) + Legal Fees = Regulatory Risk Cost

Turning Cost of Inaction into ROI

The ROI of an Abuse Desk is largely a function of risk reduction and cost savings. The same formulas that quantify the cost of inaction can be flipped to show the financial benefit of proactive abuse management. Here, the formulas remain structurally similar but are now flipped to reflect a positive budgetary impact instead of a loss.

Example:

- **Customer Churn:** Instead of lost revenue from customers leaving, calculate retained revenue from reduced churn:
  (Churn Rate Reduction Due to Abuse Desk × Total Customers) × Avg. Revenue per Customer = Revenue Retained

- **Support Costs:** Rather than additional expenses from abuse-related tickets, quantify the savings from fewer escalations:
  (Reduction in Abuse Tickets per Month × Avg. Handle Time) × Support Hourly Rate = Support Cost Savings

- **Regulatory and Legal Risk:** Instead of fines and legal fees incurred, measure costs avoided by compliance adherence:
  (Fines Avoided + Legal Fees Prevented) = Regulatory Cost Savings

- **Infrastructure and Deliverability:** Rather than increased costs from abuse, track operational efficiency gains and revenue protection:

(Reduction in Abusive Traffic x Total Hosting/Network Costs) + (Reduction in Blocklist Incidents x Revenue Loss per Incident) = Infrastructure & Deliverability Savings

- **Net Financial Recovery** is a measure of direct infrastructure expenses an Abuse Desk eliminates by preventing abuse and bad actors before they become a cost center by consuming resources.
  (Gross Cost of Abusive Infrastructure x Estimated Run Time) — Total Mitigation Cost

Every business faces unique challenges when it comes to abuse, and there's no one-size-fits-all formula for measuring its monetary impact. However, by breaking down costs into tangible areas such as customer churn, support overhead, infrastructure strain, and compliance risks, companies can quantify the actual cost of inaction.

Likewise, ROI calculations follow the same logic but shift the focus to efficiency gains, cost reductions, and revenue protection. The key is identifying the right metrics for your business and using these frameworks to make a compelling, data-driven case for investment.

Also, there is no time like now to engage your internal data partners, whether that's your analytics, operations, or engineering team. If this data isn't available yet, work with your data partner to see if they can collect it so you can start building these calculations. Help them out by clearly outlining the specific data points you'll need to calculate impact, such as abuse ticket volumes, customer churn, infrastructure costs, or revenue per user. Bringing them in early not only accelerates your analysis but also ensures alignment on how the Abuse Desk's success will be measured going forward.

Operational and Staffing Considerations

When building an Abuse Desk, it's essential to consider both the financial investment and the resources necessary for long-term success. Abuse Desks often manage a range of responsibilities, from DMCA takedowns, subpoena fulfillment, and compliance actions to industry relations and deliverability actions. While the core mission remains the same—fighting abuse—the scope of duties will vary depending on the organization. Understanding the personnel, tools, and training required to manage these diverse tasks is crucial for those looking to justify a sustainable and efficient Abuse Desk operation. Below are a few you might consider:

1. Staffing Needs

The Abuse Desk is typically composed of a variety of roles depending on the size and complexity of the organization. At a minimum, you'll likely need:

- **Abuse Analysts**: Front-line or second-tier personnel responsible for investigating and handling abuse issues.
- **Support Staff**: For larger organizations, additional support staff may be required to assist in ticket triage, provide customer support related to abuse issues, and direct abuse escalations.
- **Legal and Compliance Experts**: A legal or compliance officer is essential, especially for handling regulatory concerns like GDPR, CCPA, CAN-SPAM, CASL, DMCA, and other regulatory requirements in effect around the world.

Other roles often found under the Abuse umbrella:

- Technical Specialists
- Customer Success Managers
- Incident Response Specialists
- Consultants and/or Advisors
- Reporting and Analytics Experts
- AI and Abuse Engineers

2. Tools and Technologies

Effective Abuse Desk operations rely on having the right tools to manage cases, track abuse reports, and communicate with stakeholders. There is a wide variety of tools and technologies available, ranging from third-party solutions to in-house developed systems, each designed to address specific needs. Whether you're using ticketing systems, spam filters, compliance tracking software, or custom-built platforms, the right combination of tools is critical to maintaining operational efficiency. Common high-level considerations:

- **Ticketing Systems**: Platforms for tracking abuse cases, assigning tasks, and maintaining audit trails.
- **Monitoring Tools**: Tools to detect and track abuse, such as anti-spam, phishing, and bot detection systems.
- **Reporting and Analytics Platforms**: These help track trends in abuse, measure resolution times, and report on key performance indicators (KPIs) for ongoing improvement.
    - **KPIs to consider**: This list is just a sampling of potential KPIs to consider and should not be thought of as exhaustive. The right KPIs for your business are the ones that measure actual harm and its cost, while allowing you to set goals to decrease the cost of mitigation and revenue loss.
        - **Abuse case volume**: New cases per month, split by category and severity.
        - **Time to mitigate**: Median hours from case open to first effective containment action, by severity.
        - **False-positive harm**: Confirmed incidents where our own controls blocked or degraded legitimate mail; count, customers affected, time to clear.
        - **Compromised accounts**: Confirmed compromises per month and median time from detection to containment.
        - **Recidivism rate**: Percentage of enforcement cases where the same account/tenant had a prior case within 180 days.
        - **Abuse-attributed cost**: Hours other teams (Support, Engineering, Ops) spend on abuse work each quarter, cost at loaded rates.
        - **Emergency action frequency**: How often we use act-first paths (emergency blocks, rollbacks), as a control-health signal.

3. Training and Development

Abuse Desk personnel require specialized training to be effective. Ongoing education ensures that the team is up to date with the latest abuse trends, regulatory changes, and internal processes. Some areas of training are:

- **Abuse Investigation Training**: Ensuring staff are trained in identifying phishing attempts, spam, malware distribution, and overall poor customer performance.
- **Regulatory Compliance**: Training on current data protection laws, anti-spam legislation, and other industry regulations.
- **Customer Service and Communication**: Training on best practices for communicating with impacted customers and responding to complaints efficiently.

4. Scalability

As abuse continues to evolve, so must your Abuse Desk. Consider how your staffing and tooling will need to be scaled as the organization grows or as the volume of abuse cases increases. This means:

- **Flexible Staffing**: Constructing hiring plans (full-time, temporary, or third-party) to ensure that the Abuse Desk can accommodate seasonal demand or unexpected spikes in abuse.
- **Cloud-Based Tools**: Leveraging cloud-based systems to allow for easy scaling of infrastructure without high on-prem or upfront costs.
- **Automation**: Implementing automated workflows and ticketing systems to manage repetitive tasks and free up resources for more complex cases.
- **AI**: Using AI to augment analyst capacity and accelerate decision-making across the abuse lifecycle. Specific use cases include abuse signal correlation and anomaly detection across large datasets; automated triage and scoring of incoming reports to prioritize high-risk cases; LLM-assisted response drafting for customer-facing communications; and pattern recognition to proactively identify emerging abuse campaigns before they reach critical volume. AI does not replace human judgment in nuanced cases but materially reduces the time required to reach a well-reasoned decision. While AI contributes to prioritization or enforcement decisions, organizations should consider confidence thresholds, auditability, false-positive monitoring, human escalation/review, and additional safeguards for actions that materially affect legitimate customers.

Presenting Your Business Case

Once your business case is built, the next challenge is delivering it in a way that drives action. A compelling presentation isn't just about sharing information; it's about making the case impossible to ignore.

The most effective presentations don't just rely on data; they use storytelling to create urgency and make the problem tangible for decision-makers. By framing the case in a way that resonates emotionally and logically, you increase the likelihood of securing buy-in. All the charts in the world will be completely dismissed if you can't answer the basic question of why the executive should care if the company is still making money. Telling a meaningful story is a key skill—you should practice the presentation multiple times with different audiences before your pitch to the executives as an exercise in narrative sharpening and tuning.

1. Presentation Suggestions

The list below outlines suggestions to create engaging and impactful presentations:

- **Keep it concise.** Decision-makers often don't have time for deep dives. If appropriate, lead with key insights and/or a one-page executive summary. Supporting details may need to be kept in reserve depending on your audience. There are times when you'll need to be ready to summarize your case in a few slides or talking points. Be prepared by having multiple versions of your presentation at the ready.
- **Make it visual**. Instead of long reports or dense spreadsheets, use infographics, charts, graphs, and bullet points or a concise case study to highlight key takeaways. A simple and creative slide deck can help decision-makers quickly grasp the most critical points. Consider using an appendix for denser materials or double-click into data if necessary. Remember, meetings with executive stakeholders are a cost unto themselves; use the time wisely.
- **Anticipate objections**. Be prepared for pushback on costs, resources, or competing priorities. Have solutions ready to demonstrate your preparedness and expertise.
- **Offer a path forward**. If immediate approval isn't feasible, propose a phased rollout, pilot program, or cost-sharing model to assess the impact before full investment.
- **Make it actionable.** End with specific, named next steps—not just "Let's follow up," but "I'd like to schedule a 30-minute working session with Finance and Legal by [date] to align on the cost model." Wherever possible, give the initiative a name. Named initiatives— "Project Shield," "the Trust & Safety Foundation," "Operation Clean Slate"—give people something concrete to rally around, reference in future meetings, and take ownership of. A project with a name feels like a real program; a nameless ask feels like overhead. Combine the name with a one-page summary and a defined decision date, and you transform an open-ended request into a motion that is easy for decision-makers to say yes to.

2. Reading the Room

Preparation carries you into the room; situational awareness carries you through it. Watch for early signs that the conversation is drifting: executives checking devices, side conversations, or a shift toward cost-focused questions before you have finished framing the problem. These are signals to compress, not accelerate.

Know in advance which two or three points are non-negotiable and which supporting details you can cut or defer to a follow-up. If the room pushes back on full funding, be ready to pivot immediately to your tiered model. Presenting a phased or minimal investment option is not a concession; it is a strategic choice that keeps the conversation moving forward. Close every meeting with a defined next step: a follow-up date, a named decision-maker, or a specific question you will come back with an answer to. Consider employing a standard project management tool such as a RACI matrix to establish roles and responsibilities. Ambiguity at the end of a presentation rarely resolves in your favor.

Conclusion

Building a business case for an Abuse Desk requires more than just presenting numbers; it's about clearly demonstrating the tangible impact an Abuse Desk can have on your organization. By highlighting the cost of inaction, illustrating the potential ROI, and mapping out the necessary resources, you can provide

decision-makers with the evidence they need to act. The most effective next step is a concrete one: identify your primary executive sponsor, run one cost-of-inaction calculation using your own data, and schedule the first conversation. The frameworks in this document give you the structure — your organization's own numbers give it credibility.

References

The following sources were used to provide supporting industry data and metrics.

1. StationX. (2026). *Phishing statistics 2026: Latest attack data & trends*. https://app.stationx.net/articles/phishing-statistics
   Anti-Phishing Working Group (APWG). (2026). *Phishing activity trends report 2025*. https://apwg.org/trendreports
2. Kaspersky. (2026). *Kaspersky reports 15% growth in malicious email attacks in 2025*. https://www.kaspersky.com/about/press-releases/kaspersky-reports-15-growth-in-malicious-email-attacks-in-2025
3. Palisade. (2025). *Email security threats and statistics 2025*. https://www.palisade.email/resources-post/email-security-threats-and-statistics-2025
4. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2025). *Internet crime report (referenced statistics)*. https://bitsfrombytes.com/phishing-statistics-2026-all-datas-informations/
5. SSL Insights. (2026). *Phishing statistics: Key data, trends, and emerging threats*. https://sslinsights.com/phishing-statistics/
6. Kickbox. (2025). *Email deliverability report: The cost of missing the inbox*. https://kickbox.com/resource-center/email-deliverability-report
7. Atlas VPN (citing Egress survey). (2023). *Survey: 92% of organizations fell victim to phishing in the last 12 months*. https://tdwi.org/articles/2023/03/22/survey-phishing-attacks.aspx
8. Validity. (2025). *Email deliverability benchmark report*. https://www.validity.com/wp-content/uploads/2025/03/2025-Benchmark-Report-FINAL.pdf
9. Braze. (2024). *Deliverability indicators: Understanding email blocklists and their impact*. https://www.braze.com/resources/articles/deliverability-indicators-understanding-email-blocklists
10. DeepStrike. (2025). *Phishing statistics and breach lifecycle analysis*. https://deepstrike.io/blog/Phishing-Statistics-2025

As with all documents that we publish, please check the M[3]AAWG website (www.m3aawg.org) for updates.

© 2026 Messaging, Malware and Mobile Anti-Abuse Working Group (M[3]AAWG) M3AAWG-160