CISO GUIDE TO

Defending the Brand

Key Strategies for Comprehensive Online Brand Protection

FORTRA™

Cybersecurity INSIDERS

The Critical Importance of Online Brand Protection

As the digital landscape expands, so do the risks associated with it. The proliferation of online platforms—such as social media, websites, e-commerce sites, and mobile applications—has created unprecedented opportunities for brands to engage with their audiences.

However, these opportunities have also exposed vulnerabilities, with threat actors leveraging advanced tactics, including AI-enhanced methods, to impersonate brands, conduct online phishing attacks, and infiltrate nontraditional channels like online marketplaces and the dark web.

Social media platforms like X, TikTok, LinkedIn, and Instagram, have become major threat vectors for brand impersonation, phishing attacks, and counterfeit campaigns. Attackers also exploit repositories like GitHub and discussion forums like Reddit, using these less traditional channels to launch fraudulent campaigns. The rise of these tactics underscores the need for a more advanced and comprehensive approach to brand protection.

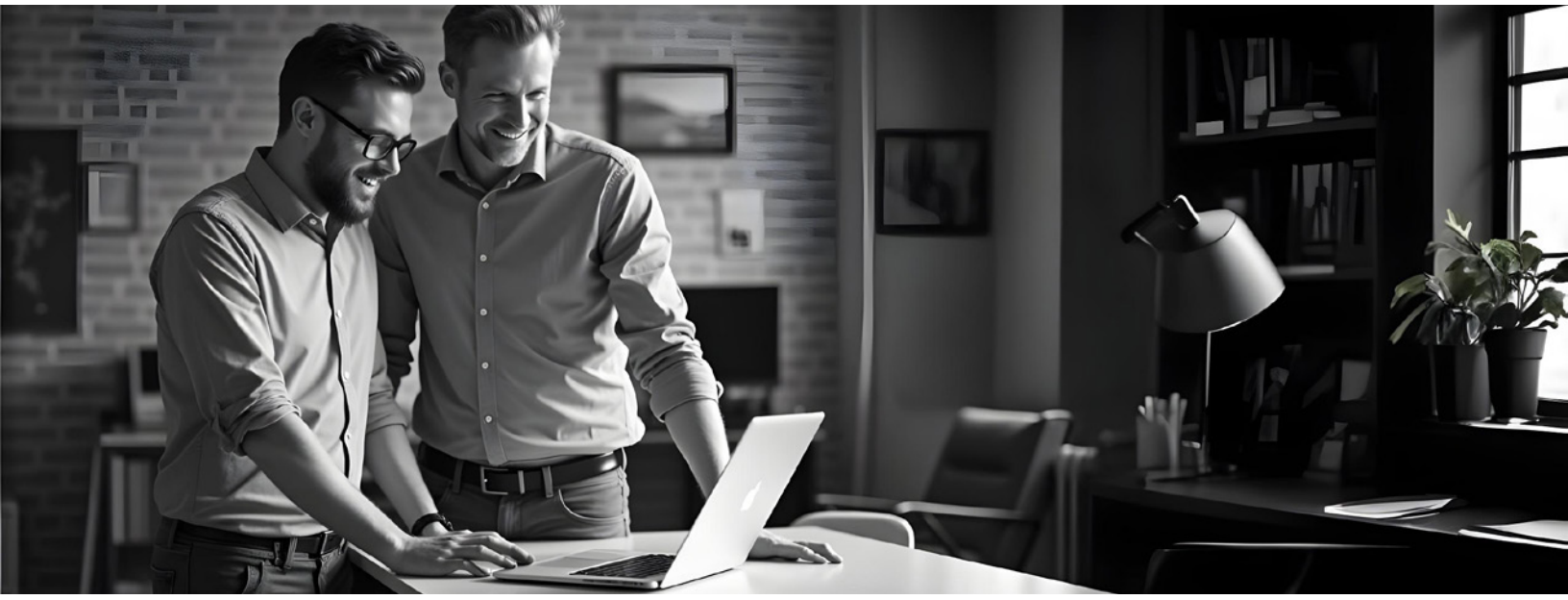
Neglecting robust brand protection can lead to significant financial losses, regulatory penalties, and long-term reputational damage. Studies show that two-thirds of consumers would switch providers after a fraud incident, underscoring the urgency of implementing robust brand defenses.

To effectively counter these threats, Chief Information Security Officers (CISOs) must implement a range of proactive measures, including domain ecosystem monitoring to detect look-alike domains, social media protection to identify fake profiles or fraudulent ads, and counterfeit detection across online marketplaces. These strategies ensure comprehensive protection by safeguarding brand identity, preventing online phishing attacks, and removing counterfeit products that could harm customer trust.

For example, automated detection systems such as those offered by Fortra, paired with human expertise in curation, can filter out false positives and prioritize actionable threats, allowing security teams to focus on high-risk incidents. Collaboration with platforms, IP enforcement, and the use of real-time threat intelligence are crucial components of these efforts as well.

To maintain the effectiveness of these strategies, CISOs must also track key performance indicators (KPIs) like incident detection rates, response times, and the success of takedowns. By leveraging tools that incorporate advanced mitigation techniques, such as Fortra's automated killswitches and takedown APIs, which enable quick removal of fraudulent domains and counterfeit sites, organizations can, for example, significantly reduce the window of exposure to brand threats. Continuous evaluation of these metrics allows organizations to stay ahead of evolving threats, protecting both financial stability and customer trust.

For Chief Information Security Officers, digital brand protection is no longer just a marketing concern but a core component of the organization's overall security strategy. The complexity of cyber threats demands cross-departmental collaboration with security teams, marketing, legal, and customer-facing teams working together to ensure comprehensive brand protection.



FORTRA

Common Challenges in Managing Brand Protection

Managing digital brand protection is a complex task that requires visibility across a wide range of online channels, rapid detection of threats, and the ability to mitigate incidents quickly. Many organizations struggle to achieve this due to the sheer volume of data across a multitude of platforms, the fast-paced evolution of online threats, and the lack of budget and specialized expertise in handling brand-specific risks.

Digital Risk Expansion

The scope of digital brand risks has grown significantly, extending beyond traditional threats like website impersonation and counterfeit goods. Today, social media plays a central role in brand fraud. Attackers exploit established platforms like Facebook, Instagram, LinkedIn, and X (formerly Twitter), as well as newer, less regulated platforms such as TikTok. These platforms enable cyber criminals to create impersonation accounts, launch phishing attacks, and promote counterfeit products, which all harm a brand's reputation, defraud organizations, and erode consumer trust.

A key challenge for security teams lies in the vast number of platforms that must be monitored. Traditional networks demand constant attention, but newer, fast-evolving platforms present unique risks.

For instance, TikTok's short-form video format enables attackers to distribute fraudulent content quickly to large audiences, while Telegram's private, encrypted channels provide cover for illicit activities, including phishing and counterfeit goods trading.

To protect their brand effectively, organizations must adopt a multi-platform monitoring strategy that leverages advanced detection tools to identify threats across domains, social media platforms, and even repositories like GitHub. This complexity highlights the importance of cross-platform defenses to address evolving threats.

In addition to investments in brand protection solutions, effective brand defense requires an organizational shift in how responsibilities are handled, particularly between security and marketing teams. A collaborative approach can bridge the gaps and ensure that brand protection is comprehensive and consistent.

The Evolving Role of the CSIO in Brand Protection

Traditionally, brand protection was considered the domain of marketing teams, focused on managing reputation and engaging with customers. However, as digital threats have escalated—ranging from social media impersonation and intellectual property theft to domain spoofing and counterfeit campaigns—the responsibility has expanded to security teams.

Today, CISOs are increasingly involved, recognizing that brand protection is not just a marketing issue, but a vital aspect of the organization's overall security strategy.

One of the key challenges in this transition is the lack of clarity around responsibilities between marketing and security. Marketing teams are adept at handling brand visibility and customer sentiment, especially on social media, but they typically lack the technical expertise to identify and mitigate cyber threats like, fake profiles, ads for counterfeit products, or phishing websites. This gap leaves organizations exposed to evolving threats. Meanwhile, cybersecurity teams possess the necessary tools and expertise but often lack visibility into marketing-managed activities, such as social media monitoring.

This fragmentation can lead to slower threat responses, particularly across digital channels, and increases the organization's vulnerability to brand-related risks.

As the digital landscape continues to evolve, so does the role of the CISO. No longer limited to IT security, CISOs now play an essential role in ensuring the organization's overall trust and market reputation. This shift from a purely technical role to one that aligns security with broader business goals positions the CISO as a strategic leader within the organization. Today, CISOs must not only protect internal IT infrastructure but also safeguard the organization's brand and customer relationships, addressing external threats that span a wide range of platforms and third-party services.

Financial & Reputational Cost of Inaction

Failing to address brand-related fraud effectively can have severe financial, reputational, and legal consequences. The impact of inaction is twofold: direct financial losses due to fraudulent activities and reputational damage that leads to customer churn and diminished trust. Both consequences are closely intertwined, with financial costs often exacerbated by the long-term reputational effects.

▶ Erosion and Loss of Customer Trust

Brand impersonation—whether through phishing websites, counterfeit products, or fake social media profiles—severely undermines customer trust. Consumers expect to interact with legitimate entities, and falling victim to impersonation scams causes a breach of this trust.

A study by PwC found that 85% of consumers would not do business with a company if they had concerns about its security practices.

Furthermore, nearly two-thirds of consumers are willing to switch providers after experiencing fraud, leading to significant customer churn and long-term damage to brand loyalty.[1]

▶ Direct Financial Losses

When brands are impersonated, especially on social media platforms or look-alike websites, cybercriminals can steal funds or sensitive information from customers. A Juniper Research study estimated that brand fraud costs businesses over $5.2 trillion globally between 2019 and 2024 due to losses from fraudulent transactions and customer redress expenses. These costs include refunds to defrauded customers, legal fees, and expenses related to fraud detection and mitigation efforts.[2]

▶ Penalties and Fines

Many industries are subject to regulatory penalties when fraud or impersonation compromises customer data. For example, under regulations such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) organizations may face substantial fines if they fail to protect customer data. Recently, British Airways was fined £20 million by the UK's Information Commissioner's Office after a data breach involving fraudulent websites compromised the personal information of 400,000 customers.[3]

▶ Costs of Customer Remediation

After an impersonation or fraud incident, brands often need to offer remediation, such as refunds or identity theft protection services, to affected customers. According to IBM's Cost of a Data Breach Report, the cost to resolve fraud-related issues can range from $200 to $400 per incident, quickly escalating into millions for large-scale incidents.[4]

▶ Customer Churn and Lost Business

The impact of fraud on customer retention can be severe. A Cisco survey revealed that 29% of consumers will stop interacting with a brand entirely after experiencing fraud, even if the company takes steps to remediate the issue. This churn results in significant lost business, which can be particularly damaging in competitive markets where acquiring new customers is costly.[5]

▶ Long-Term Reputational Harm

Beyond immediate financial loss, the long-term reputational harm caused by brand fraud is much harder to repair. Negative publicity can linger for years, reducing market share and making it harder for brands to attract new customers. According to a report from Deloitte, companies that fail to protect their digital presence can experience a 15% to 20% drop in brand value after a major fraud incident.[6]

To avoid these steep costs, organizations must invest in robust brand protection strategies, ensuring that their digital presence is secure across all platforms. By addressing the threat of brand fraud proactively, businesses can safeguard both their financial stability and long-term reputation.

FORTRA

Proactive Defense Strategies and Best Practices

In today's hyper-connected world, CISOs require more than just basic monitoring tools to effectively defend against brand-related cyber threats. Solutions like Fortra's that offer a combination of broad, automated detection, expert curation, and rapid mitigation play a pivotal role in stopping critical threats before targeted campaigns can cause significant damage.

Proactive defenses involve ongoing monitoring, identifying brand-specific vulnerabilities, and leveraging best practices to mitigate risks such as social media impersonation, fraudulent ads, and domain spoofing. By implementing preemptive strategies, CISOs can ensure comprehensive, forward-thinking protection that mitigates brand fraud risks while preserving the organization's reputation.

Identifying Brand-Specific Cyber Threats

A crucial first step for CISOs is to identify the specific brand vulnerabilities their organization faces, as these threats can vary depending on the industry and brand exposure.

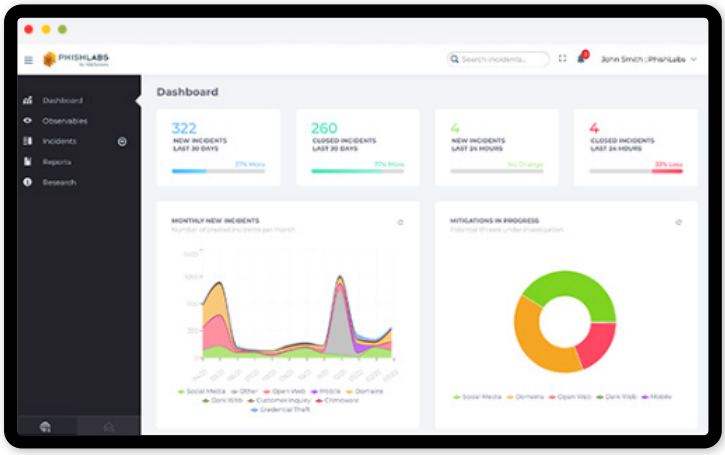
Common risks include:

- **Social media threats:** Impersonation of company profiles or executives and the spread of fraudulent ads.
- **Domain abuse:** Spoofedor look-alike domains that deceive customers and facilitate phishing.
- **Website impersonation:** Fake sites designed to mimic legitimate brands, steal customer information, or sell counterfeit products.

Understanding these brand-specific threats is essential for tailoring an effective defense strategy. For instance, finance and retail sectors are more likely to encounter phishing sites and domain spoofing, while brands with a heavy social media presence are vulnerable to social media impersonation and ad fraud.

Domain Ecosystem Monitoring

One of the most critical proactive measures is monitoring the entire domain ecosystem, not just the domains an organization owns. Cybercriminals frequently register look-alike domains or typo-squatted versions of official websites to trick customers into believing they are interacting with legitimate brands. These domains are often used for phishing or malware distribution.



Key monitoring elements include:

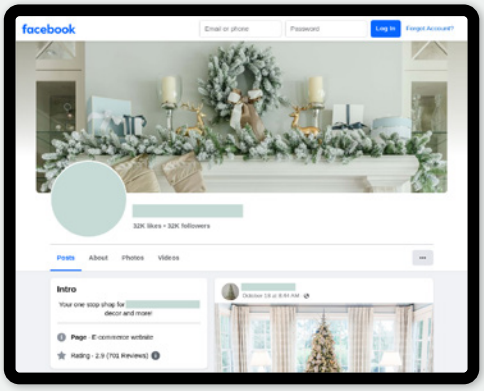
- Tracking newly-registered domains resembling your brand name.
- Monitoring SSL certificates to prevent fake sites from acquiring legitimate-looking credentials.
- DNS monitoring to catch unauthorized changes in MX records or WHOIS data that might indicate domain hijacking.

Using a full-service monitoring solution allows security teams to detect suspicious domain activity early and ensure the swift takedown of a wide variety of domain threats

Social Media Protection

Given that over 5 billion users globally have been active on social media platforms in 2024, monitoring must go beyond popular platforms like Facebook, Instagram, LinkedIn, and X . Attackers are now exploiting newer platforms, such as TikTok, Telegram, and even repositories like GitHub, to launch fraudulent campaigns or impersonate brands. Additionally, gripe sites and forums like Glassdoor and Reddit can become vectors for misinformation and brand abuse.

Comprehensive social media protection is essential for safeguarding a brand's digital presence. Advanced detection tools that can score and rankpotential threats, combined with expert human curation, are crucial to differentiating real risks from the overwhelming amount of social media data.



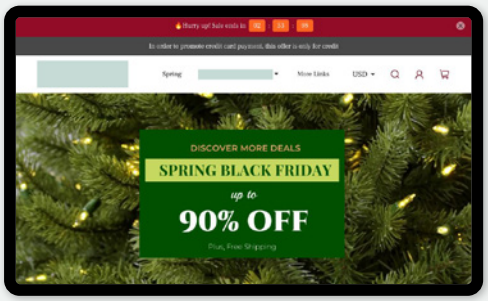
Best practices for social media protection include:

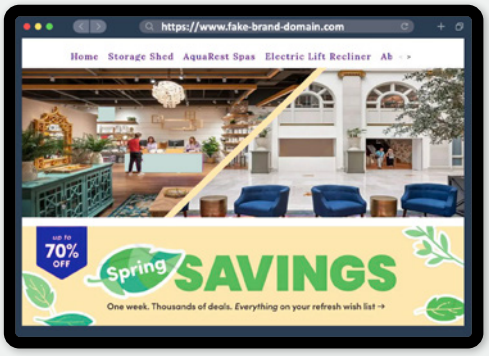
- Creating and verifying official profiles for your brand and key executives to establish authenticity. If these profiles are left unclaimed, attackers can easily fill the void.
- Monitoring activity across all social media platforms, including emerging ones. This allows you to catch fake profiles, impersonations, or fraudulent ads before they cause widespread damage.
- Filtering real threats from the noise using advanced detection tools that automate the process of scoring threats and validating results with human curation.
- Adjusting workflows based on threat severity. Allocating resources efficiently requires prioritizing incidents by risk level. For example, physical threats to executives demand faster escalation than lower-priority threats.
- Understanding who is most at risk—identifying high-value targets, such as executives, influencers, VIPs, or brands, that attackers are more likely to impersonate.
- Informing employees and customers regularly about ongoing threats and best practices to protect themselves from scams involving your brand.
- Registering your brand's trademarks on social media platforms and considering legal protections to help facilitate takedowns and counter fraud.

Without proactive social media monitoring, organizations risk missing threats, resulting in delayed responses and costly brand damage.

Counterfeit Protection

Counterfeit products and fraudulent ads are significant threats to brands, particularly on e-commerce platforms and social media. Cybercriminals use look-alike domains, fake storefronts, and competitive paid ads to divert revenue and erode customer trust. To combat these activities, continuous monitoring of digital channels is essential. Tools that score and categorize counterfeit activities can help prioritize responses based on the severity of the threat.





Key proactive measures for counterfeit protection include:

Automated detection systems:
Employ advanced tools to identify counterfeit ads, look-alike domains, and unauthorized use of brand assets across digital platforms.

Human curation:
Assign prioritized threats to experts for validation and action.

Domain and social media monitoring:
Actively monitor for fake listings or unauthorized product advertisements, particularly across high-traffic sites like e-commerce platforms and social media.

Strong partnerships with platforms:
Establish relationships with digital platforms (such as social media platforms, domain registrars, web hosts, and app stores) to streamline takedown processes and quickly remove counterfeit storefronts or fraudulent content.

Real-time threat intelligence:
Continuously update security teams with the latest information on counterfeit tactics and trends to stay ahead of emerging threats.

Enforcement of IP rights:
Ensure trademarks and copyrights are registered and enforceable on digital platforms, allowing for quicker takedown and legal action when necessary.

By integrating these practices into their brand protection strategies, CISOs can mitigate financial losses and reputational damage caused by counterfeit activities.

Creating a Security-Aware Culture

Another cornerstone of proactive defense is establishing a security-aware culture across the organization. Brand protection is not solely a marketing or cybersecurity responsibility—it requires collaboration across all departments. Security training must extend to all teams, including marketing, legal, and customer service, focusing on:

- **Social media best practices for employees to identify impersonation attempts and report suspicious activity.**
- **Intellectual property (IP) protection to ensure employees understand the risks of unauthorized use of brand assets.**
- **Incident response plans that outline how teams should react to brand-related threats and fraud incidents.**

By implementing these proactive defenses—from domain ecosystem monitoring to social media protection and creating a security-aware culture—CISOs can safeguard their brand from a wide range of digital threats.

Ongoing vigilance and cross-functional collaboration between security, marketing, and other teams are essential for a comprehensive defense strategy that evolves with the changing digital landscape.

FORTRA

Measuring the Effectiveness of Brand Protection Efforts

To ensure that brand protection strategies are not only effective but continually improving, continuous evaluation is critical. CISOs need to track key performance indicators (KPIs) that provide insight into how well their defenses are mitigating risks, preventing fraud, and maintaining the integrity of the brand.

Below are the essential KPIs that organizations should monitor to assess the success of their brand protection efforts throughout the lifecycle of threat detection, response, and impact assessment:

01. Incident Metrics

(Measuring Threat Detection)

The first step in the brand protection lifecycle is identifying and reporting brand-related threats. Incident metrics track the volume of incidents, providing insight into the types and frequency of threats, such as fraudulent websites, social media impersonations, or online phishing attacks.

▶ What It Tells:

Incident metrics highlight the scope and diversity of threats, revealing which platforms or channels are most vulnerable. If detection rates are high but mitigation rates are low, this may indicate resource constraints or ineffective enforcement mechanisms.

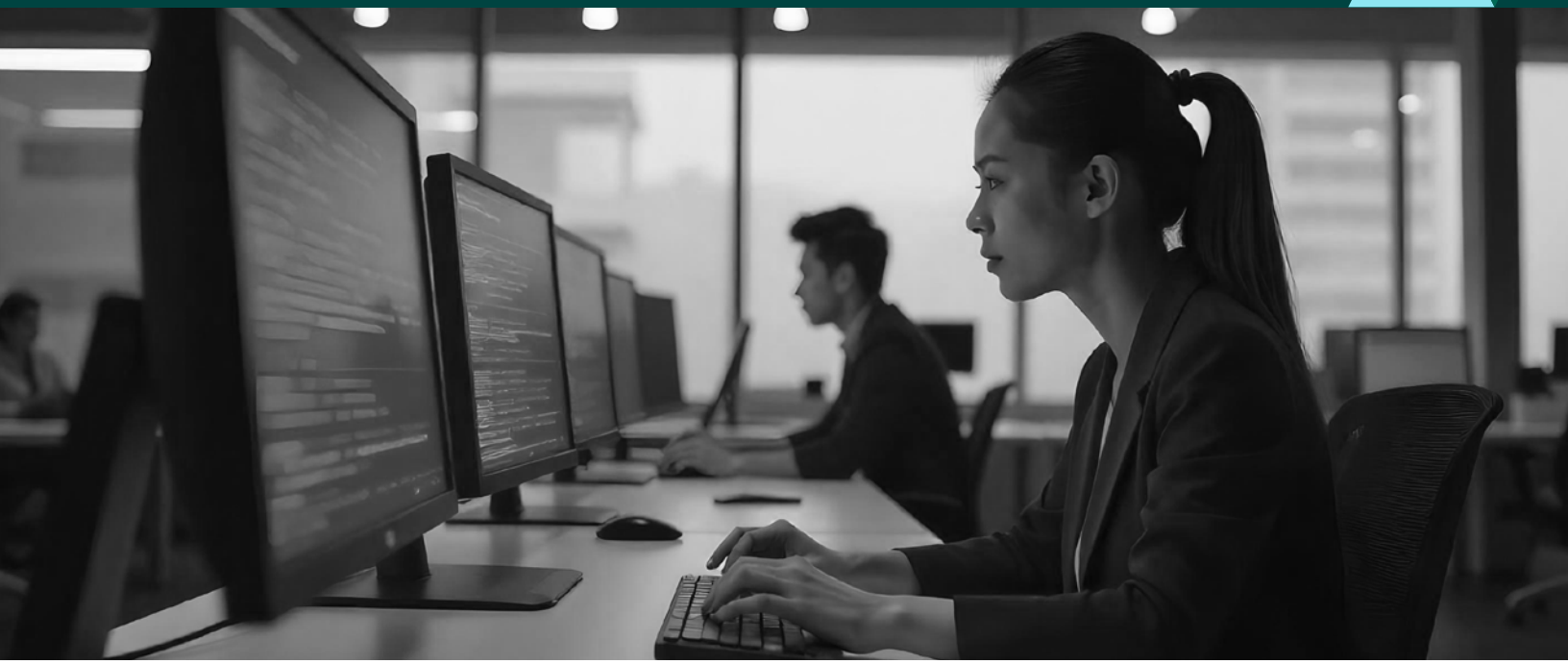
▶ How to Measure:

Use tools that log reported incidents, categorize them by severity, and track them through the entire lifecycle—from identification to resolution. Monitoring these metrics over time helps assess the evolution of risks and protection efficacy.

02. Speed to Impact

(Measuring Response Efficiency)

After a threat is detected, the speed of response becomes critical. The faster your team can mitigate a threat—whether through takedowns or legal enforcement—the less opportunity it has to cause financial or reputational damage.



▶ What It Tells:

Speed to impact can reflect the efficiency of response workflows. A faster time-to-action reduces exposure and demonstrates organizational agility in handling threats.

▶ How to Measure:

Track timestamps from the moment a threat is detected to the point it is resolved or use tools that calculate this metric. Comparing response times across different threat types allows for workflow optimization and highlights areas where additional resources or tools are needed.

03. Takedown Rate

(Measuring Mitigation Success)

Once a threat is detected, the next step is to remove it. Tracking the number of confirmed threats vs. takedowns achieved—whether for fraudulent websites, social media profiles, or counterfeit ads—reveals the success rate of your mitigation efforts.

▶ What It Tells:

This metric indicates how well your brand protection strategies are working. A higher takedown rate shows both the volume of threats being tackled and the effectiveness of your team in neutralizing risks.

▶ How to Measure:

Track and categorize the takedown rate of confirmed malicious incidents (based on Terms of Service violations) over a given period. This ensures that the most significant threats are being addressed effectively.

Expert tip: *Learning which evidence is needed for takedown, which varies across service providers, can vastly improve takedown rate and speed.*

04. Customer Feedback

(Measuring Post-Mitigation Impact)

While removing threats is crucial, assessing their impact on customer perception is equally important. Customer feedback helps measure how brand protection efforts affect customer experiences and brand trust.

▶ What It Tells:

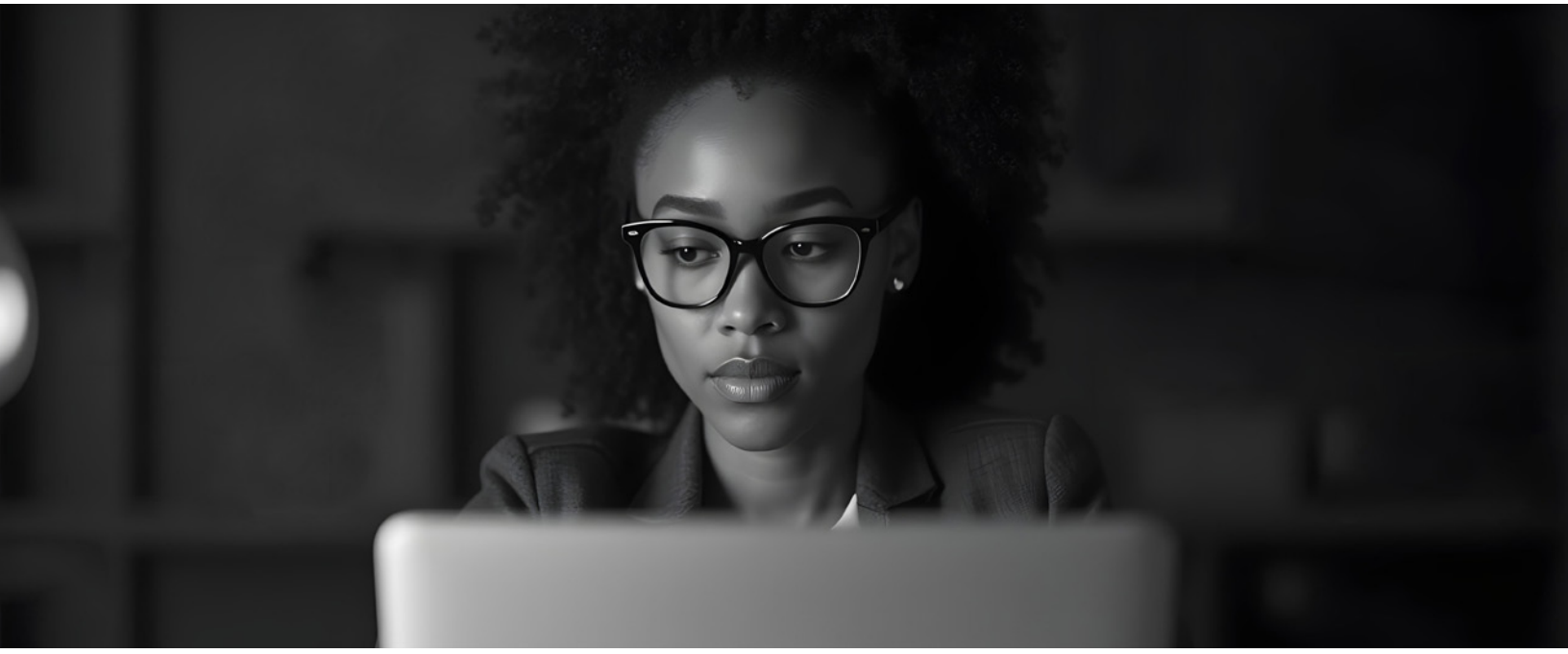
Customer feedback is a direct reflection of brand health. Positive feedback suggests effective brand protection strategies, while an increase in fraud-related complaints indicates areas for improvement.

▶ How to Measure:

Monitor customer surveys, social media mentions, and inquiries related to fraud or impersonation. Track the volume of complaints and feedback over time, comparing it to pre- and post-implementation of brand protection measures.

By focusing on these KPIs, CISOs can build a clear picture of how well their brand protection efforts are performing. The number of takedowns highlights how active the threat landscape is for your brand. Incident metrics and speed to impact provide detailed insights into your team's efficiency, while customer feedback offers a broader view of how well customers perceive your brand.

Monitoring these KPIs on a continuous basis ensures that your organization is staying ahead of emerging threats and maintaining both customer trust and brand integrity. Moreover, regular evaluation of these metrics allows organizations to refine their defense strategies and adapt to the constantly evolving digital threat landscape.



FORTRA

CONCLUSION: The Role of CISOs in Safeguarding the Brand

In today's rapidly evolving digital landscape, CISOs are at the forefront of defending their organization's online presence and reputation. The responsibility for brand protection has shifted from being primarily a marketing function to becoming a core component of the cybersecurity strategy. With the rise of sophisticated brand-related cyber threats, including social media impersonation, domain spoofing, and counterfeit ads, CISOs must lead a unified, comprehensive defense approach that extends beyond IT infrastructure.

Through proactive monitoring, identifying brand-specific vulnerabilities definining an established, clear way to mitigate threats quickly, and building cross-functional defenses, CISOs ensure that brand fraud is detected and mitigated before it can cause severe financial, legal, or reputational damage.

The integration of tools like Fortra'sPhishLabs—combining broad detection, expert threat curation, and the rapid mitigation of threats—provides a crucial defense mechanism for recognizing critical threats and reducing exposure time.

Key defense strategies, such as domain ecosystem monitoring, social media threat detection, and counterfeit protection, are no longer optional but vital components of a holistic cybersecurity framework.

These strategies work together to protect both customer trust and organizational stability by preventing the exploitation of look-alike domains, online phishing campaigns, and misleading ads across multiple platforms.

To ensure continuous effectiveness, CISOs must measure the success of these brand protection strategies through KPIs.

Metrics such as incident detection rates, response times, and takedown success rates provide actionable insights that allow organizations to refine their defenses and adapt to emerging threats.

Moreover, tracking customer feedback offers an invaluable perspective on how well brand protection efforts resonate with consumer trust and satisfaction.

Ultimately, the modern CISO is not just a guardian of internal IT infrastructure but a strategic leader responsible for safeguarding the organization's most valuable asset—its brand reputation. By fostering cross-departmental collaboration with marketing, legal, and customer-facing teams, investing in advanced detection tools, and maintaining continuous vigilance, CISOs ensure their organizations are equipped to navigate the ever-expanding cybersecurity landscape. This proactive, collaborative approach not only preserves organizational stability but also secures long-term profitability and customer loyalty in a world where digital threats continue to grow in complexity.

[1] **Source:** PwC Australia. *"Protect.me: How consumers see cyber security and privacy risks."*
Available at: https://www.pwc.com.au/digitalpulse/report-protect-me-consumers-cyber-security.html

[2] **Source:** Accenture. *"Cybercrime Could Cost Companies US$5.2 Trillion Over Next Five Years."*
Available at: https://newsroom.accenture.com/news/2019/cybercrime-could-cost-companies-us-5-2-trillion-over-next-five-years-according-to-new-research-from-accenture

[3] **Source:** BBC News. *"British Airways fined £20m over data breach."*
Available at: https://www.bbc.com/news/technology-54568784

[4] **Source:** IBM Security. *"Cost of a Data Breach Report 2020."*
Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/

[5] **Source:** Freevacy. *"2020 Cisco Consumer Privacy Survey."*
Available at: https://www.freevacy.com/news/cisco/2020-cisco-consumer-privacy-survey/894.

[6] **Source:** Deloitte Digital. *"Personalizing growth."*
Available at: https://www.deloittedigital.com/us/en/offerings/customer-led-marketing/advertising--marketing-and-commerce/personalizing-growth.html