McAfee
Together is power.

Why Offense Beats Defense: Misaligned Incentives—A Focus on the Financial Services Sector

Cybercriminals have long had the advantage, continually finding new ways to steal data, break services and disrupt the legitimate flow of information. Not because they are better, but because of a mismatch between the incentives of attackers and defenders. To better understand this misalignment of incentives, we surveyed 200 IT professionals from the financial services industry, and compared their responses to 600 IT professionals from other global industries. The **report** identified three key incentive misalignments: between corporate structures and the free flow of criminal enterprises, between strategy and implementation, and between senior executives and those in implementation roles.

Three Levels of Misaligned Incentives Put Defenders at a Disadvantage

Attackers vs. Defenders	Attackers' incentives are shaped by a fluid, decentralized market, making them agile and quick to adapt, while defenders are constrained by bureaucracy and top-down decision making.
Stategy vs. Implementation	While more than 90% of organizations have a cybersecurity strategy, less than half have fully implemented their strategies.
Executives vs. Implementers	Senior Executives designing cyber strategies measure success differently to those who implement those strategies, limiting overall effectiveness.

Corporate Structure vs. Criminal Enterprise

The financial services industry has long understood the effects of clear and direct incentives. Cybercriminals operate in a dark but open world of freelancers and clear motivation, promoting dynamic competition and rapid innovation. This encourages a great deal of specialization, enabling elite cybercrime practitioners to become very good at their trade and creating a broad web of suppliers and customers. Information is shared through a wide range of channels and new vulnerabilities are exploited very quickly. Active markets make it easy to find interested customers and put a price on new information and code.

According to this research, financial services organizations are the closest of those surveyed to running an open information market for cyber defense. They are the most likely to share information with other organizations, including partners (63% vs. 52% of respondents from non-financial industries), outside consultants (49% vs. 39%), and even competitors (26% vs. 19%). Only 7% of those surveyed stated that they do not share any cyber-threat information, compared to 14% of those in other industries.

This attitude towards sharing influences the sources that financial services organizations use when making cybersecurity decisions. They are slightly more likely to use information that has been shared from outside sources than those in other industries. This includes intelligence from security vendors (63% vs. 57%), outside consultants (51% vs. 46%), and industry groups (26% vs. 22%). It could be that this information is being analyzed and summarized by operators, as the financial service professionals are also much more likely to use internal briefings than those in other organizations (70% vs. 61%).

Support of open markets for cybersecurity in the financial services industry extends beyond information into services and consultants. They are the most likely to spend a significant portion of their cybersecurity budget on consultants (49% vs. 40% of the non-financial organizations), and slightly more likely to spend money on professional services for monitoring and incident response (38% vs. 34%). This openness to outside information and specialists has been shown to have a positive impact on security effectiveness.

Disconnect Between Strategy and Implementation

Cybersecurity is now the number-one risk facing organizations, according to a majority of respondents across all industries. Almost 80% of financial services organizations are briefing their board of directors on cybersecurity risks at most or every board meeting, compared to just 70% of those in other sectors. While almost all (95%) of the financial industry respondents reported that their organization has a cybersecurity strategy intended to address both new and existing threats, the challenges arise mostly in implementation. Just over half (51%) of the organizations stated that they have fully implemented their cybersecurity strategy, and 8% have not implemented any of it.

Some of the disconnect in implementing security strategies may be due to a misplaced concern about the nature of the risks to the business. On average, the leadership and boards of these financial services organizations were reportedly more concerned about harm to the company's reputation (67%) than to loss of revenue or profit (50%). Given the recent surge in direct thefts from the financial industry, as opposed to fraud losses due to stolen credit card numbers, this attitude may be providing a false sense of security.

Those who are implementing their security strategy appear to have an above average level of security maturity. The highest-ranked task of these security teams was proactive defense, followed by investigating new strategies and solutions, and then reactive defense. Possibly more important, they spent the least amount of time on non-cybersecurity tasks, at just 8%, compared to 14% for those in other industries.

As an industry that has long been a target of cyberattacks, it did not come as a surprise that 73% of financial services security professionals reported that their budget was adequate to implement their strategy, compared to only 58% of the other industry sectors. Only a small number of companies in the financial industry felt that their budget (4%) or staffing (9%) was insufficient and would cause problems for their strategy implementation.

Another disconnect between strategy and implementation are the methods used to ensure that cyber-defense measures do not open the organization up to new risks. While the majority of financial firms (73%) reported that they are maintaining a security platform that integrates existing and new technologies, a similar number (70%) stated that they are also acquiring overlapping security technologies. While this may appear to be a sound implementation strategy, overlapping security technologies that are not adequately integrated can sometimes result in security gaps, as different configuration and monitoring systems make it difficult to create and enforce consistent security policies.

Different Incentives for Senior Executives and Implementers

Cybercriminals have a direct incentive for their efforts, in the form of money, publicity, or embarrassment of their target. Cybersecurity teams in financial services are most likely to have existing incentives such as recognitions (55% vs. 48% of those in other sectors) and bonuses (53% vs. 43%). Only 9% of those surveyed reported no incentives currently exist, compared to 21% in other sectors. The primary disincentive against risky cybersecurity behavior by employees is the threat of legal action (69% vs. 59%). In addition, 56% of financial industry IT professionals report that strategy implementation is incorporated into their individual performance reviews, compared to only 46% of those in other industries.

Determining if the strategy is meeting objectives requires a sufficiently detailed set of metrics. Only 1% of the financial services respondents stated that they could not determine if they were meeting objectives, compared to 7% of those in other sectors. While still not a significant majority, more of the financial cybersecurity teams reported appropriate methods for evaluating the strategy than other industries, such as risk management activities (66% vs. 57%), and mean time to resolution (52% vs. 45%).

Learning from Cybercrime

Financial services firms, with a long history of operating in various types of markets, appear to have the smallest misalignment of cybersecurity incentives. They are already the highest users of consultants and outside security services, but could possibly give more weight to external threat intelligence and security information over their internal briefings. The security processes in these teams appear to be maturing well, and they should continue to focus on integrated solutions instead of relying on overlapping security products. They may also need to increase their focus on new threats and the risk of actual financial loss over reputational loss, as attackers are increasingly looking to steal funds directly (for example, increase in mobile banking Trojans, SWIFT/Bangladesh theft, Tesco Banking compromised accounts).

Lessons from the Criminal Market	Criminal Market	Defenders' Advantage
	Crime-as-a-Service	**Security-as-a-Service**
Leverage Market Forces	The open and decentralized criminal market leverages competition and market pricing to minimize barriers to entry, foster innovation, and help successful ventures quickly achieve scale	Greater use of outsourcing and open contracting can help reduce costs, increase competition, and facilitiate the broad adoption of effective security technologies and practices.
	Target Publicly Disclosed Vulnerabilities	**Improve Patching Practices**
Use Public Disclosure	Exploiting disclosed vulnerabilities avoids costly vulnerability research and exploit development, and quickly incorporates new disclosures into attacks to maximize value before defenders patch.	Responding more quickly to public vulnerability disclosures through improved patching practices and faster replacement of legacy systems can enhance security and raise costs to attackers.
	Open Forums and Online Advertising	**Information Sharing and Collaboration**
Increase Transparency	Open forums and public advertising facilitate the proliferation of successful new attacks and criminal business models, and the widespread adoption of best practices.	Expanding information sharing can help reduce costs to defenders by reducing duplication, and can help spread the word about new technologies and practices that deliver significant improvements in security.
	"Anyone who is computer literate"	**Tap Global Talent Pool**
Lower Barriers to Entry	Lacking formal qualifications or geographical constraints, the criminal ecosystem is able to bring in undervalued talent from the legitimate economy and maximize its value.	Drawing on a broader, multinational, and demographically diverse talent pool can help fill the cyberskills gap for companies and drain talent from the criminal market.
	Freelance Markets Reward Performance	**Performance Incentives**
Align Incentives	In the freelance criminal market, operators at all levels and all functional areas of the attack chain are rewarded by the market for excellence and penalized for under performance.	In order to align incentives from leadership down to operators, incentives like awards and bonuses must be provided to employees and managers who deliver good security outcomes.

Learn More

For more details on misaligned incentives in cybersecurity, including breakdowns by country and vertical industry, download the full report, **Why Offense Beats Defense: Misaligned Incentives.**

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com