Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity

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 800 cybersecurity professionals from five major industry sectors. 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 versus 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.
Strategy versus implementation	While more than 90% of organizations have a cybersecurity strategy, less than half have fully implemented their strategies.
Executives versus implementers	Senior executives designing cyber strategies measure success differently to those who put strategies into practice, limiting their effectiveness.

Corporate structure versus criminal enterprise

While the targets of most cyberattacks are some type of organization with hierarchy and bureaucracy, cybercriminals operate in a dark, but open, world of freelancers and clear incentives. The cybercrime market responds to "price signals" with innovation and with new products and services on offer every day. When old capabilities are burned, replacements come online quickly. This enables dynamic competition and rapid innovation among the various parts of the cybercrime market—from the highly sophisticated and well-resourced criminals and nation-state-sponsored actors to the hacktivists and Cybercrime-as-a-Service consumers. For this study, we interviewed technical cybersecurity experts and law enforcement officers to gain a deeper understanding of these markets.

There is a great deal of specialization in the cybercrime markets, enabling the elite practitioners to become adept at their trade. The most common specialties are malware programmers, malicious website designers, infrastructure experts, exploit and vulnerability hackers, and con artists who devise social engineering schemes. Profits are distributed among the specialists according to their contribution. Dynamic competition and reputational information continually squeeze out the less capable criminals and draw the best ones to the top.

One of the primary effects of this direct competition and compensation model is the speed at which new vulnerabilities or exploits are used. As many as 42% of vulnerabilities are exploited by criminals within 30 days of being disclosed. For example, when the developers of the once-dominant Angler exploit kit (which made up 82% of exploit kit activity according to one estimate) were arrested, within weeks attackers who had relied on Angler adopted the Neutrino exploit kit to replace it and deliver their payloads. Most criminals do little or no research, instead taking advantage of the work of the elite criminals, which is often quickly distributed through dark web markets and the vast number of systems that take too long to be patched. This has the added effect of keeping their costs low.

Cybercrime anecdotes make it seem like many criminals are from Russia and Eastern Europe. There is some truth to this, primarily due to the advanced math and computer science programs available and the shortage of legitimate employment opportunities. Even legitimate employees of IT and telecommunications companies in these regions will often moonlight as criminals, sometimes openly posting their dark web identities on their Facebook pages. Corporate cybersecurity defense teams can learn a great deal from these dark markets. Clear incentives and reputational awards can have a significant positive impact on attitude and effectiveness.

Disconnect between strategy and implementation

Cybersecurity is now the number one risk facing organizations, according to a majority of respondents. More than 70% of directors are being briefed on cybersecurity risks at board meetings, particularly on challenges that did not even rank in the top 10 a mere six years ago. Almost all (93%) reported that their organization has a cybersecurity strategy intended to address both new and existing threats.

This is where the first misalignment begins. Many executives believe that their strategy is fully implemented across the organization, while just over 30% of the operators agree with that statement. For both groups, the primary metric of cybersecurity effectiveness is the number of breaches, but they diverge after that. Senior executives rely more on performance metrics, such as cost of recovering from a breach or return on cybersecurity spending. Operators lean more toward technical measures, such as vulnerability scans and penetration testing. More than half (54%) of the executives surveyed are more concerned about reputational impact than the actual effects of a cybersecurity incident. A significant concern is that fewer than one-third (32%) of these professionals believe that a cybersecurity incident results in a loss of revenue or profit, possibly giving them a false sense of security.

Another disconnect between strategy and implementation are the methods used to ensure that cyberdefense measures do not open the organization up to new risks. While the majority (71%) reported that they are maintaining a security platform that integrates existing and new technologies, 64% 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. Our survey shows that not only is there a lack of incentives for cybersecurity professionals, but also that executives were more confident about the effects of existing incentives than the operational staff that they are trying to incentivize.

Almost half of the operators surveyed reported that no incentives existed in their organization, more than five times the number of those in leadership roles who reported this. It could be that employees lower down in the organizational structure are unaware of performance incentives or that they don't consider the offerings to be effective. Thankfully, 65% of the professionals surveyed stated that they were personally motivated to strengthen their organization's cybersecurity defenses.

Executives who reported existing incentives for cybersecurity professionals were most likely to identify financial compensation (60%) or recognition (58%) offerings. However, non-executives reported these same incentives as 15 to 25 percentage points lower. When asked what incentives they would like to see, operators gave almost equal weight to financial compensation (63%) and recognition or awards (62%). This is consistent with other studies that show professional development opportunities to be as or more valuable than bonuses.

Learning from cybercrime

Organizations can learn from the black hat community to help correct these misalignments. Security-as-a-Service can provide the necessary flexibility to counter Cybercrime-as-a-Service operations. Specialized consultants can augment the in-house team with expertise and focused resources when necessary. Performance incentives and recognition can encourage stronger defenses and faster patch cycles. Experimentation is necessary to determine the right mix of metrics and incentives for each organization, but improving the speed and focus of defenses and better security outcomes is within reach.

Executive Summary

Lessons from the criminal market	Criminal market	Defenders' analogue
Leverage market forces	**Crime-as-a-service** 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.	**Security-as-a-service** Greater use of outsourcing and open contracting can help reduce costs, increase competition, and facilitate the broad adoption of effective security technologies and practices.
Use public disclosure	**Target publicly disclosed vulnerabilities** Exploiting disclosed vulnerabilities avoids costly vulnerability research and exploit development, and quickly incorporates new disclosures into attacks to maximize value before defenders patch.	**Improve patching practices** 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.
Increase transparency	**Open forums and online advertising** Open forums and public advertising facilitate the proliferation of successful new attacks and criminal business models and the widespread adoption of best practices.	**Information sharing and collaboration** 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.
Lower barriers to entry	**"Anyone who is computer literate"** Lacking formal qualifications or geographical constraints, the criminal ecosystem is able to bring in undervalued talent from the legitimate economy and maximize its value.	**Tap global talent pool** Drawing on a broader talent pool, including young people and foreign ICT experts that are often drawn into cybercrime, can help fill the skills gap for companies and drain talent from the criminal market.
Align incentives	**Freelance markets reward performance** 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 underperformance.	**Performance incentives** 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.

For more details on misaligned incentives in cybersecurity, including breakdowns by country and vertical industry, download the full report, Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity, Center for Strategic and International Studies (CSIS), March 2017.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

 2480_0217_exe-misaligned-tilting-playing-field
March 2017