Misaligned Incentives

Driven by market forces, cybercriminals are outpacing defenders.

Three Dimensions Of Misalignment

Misalignment of cybercrime and response is complex. It happens at multiple levels: between attackers and defenders, between strategy and implementation, and between the executive and implementer levels of an enterprise.

Get aligned. Learn from attackers.

Adapt and thrive.

Visit www.mcafee.com/misaligned for the full report.

© 2017 McAfee, LLC

FEBRUARY 2017

Agile and quick

Attackers’ incentives are shaped by a fluid, decentralized market, making them agile and quick to adapt.

More than 90 percent of organizations have a cybersecurity strategy.

Senior executives designing cyber strategies measure success differently than the implementers.

Defenders are constrained by bureaucracy and top-down decision making.

Less than half of organizations have fully implemented their strategies.

Implementers that put strategies into practice, are limited by senior executives.

Lessons From The Criminal Market

Criminal market vs. defenders’ analogue

Leverage market forces

Outsourcing and open contracting can help reduce costs, increase competition, and promote the spread of innovative best practices.

Align 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.

Increase transparency

Improving communication during and after a breach can reduce costs, as well as reduce the reputational impact associated with a breach. (e.g., a more transparent and efficient breach response will reduce cost while improving reputation).

Lower barriers to entry

Drawing on a broader talent pool, including young people and foreign ICT experts that are often drawn into cybercrime, can help fill the cyber skills gap for companies and drain talent from the criminal market.

Leverage market forces

Countermarket forces by focusing on cost-cutting and cost avoidance strategies that lower the costs of entry for companies new to the cybersecurity market.

Use public disclosure

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

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.

Ideas/money

Upper-tier cybercriminals steal ideas while lower-tier criminals steal money.

The State Of Misalignment

While cybersecurity risk is more of a concern than ever for enterprises, there are fault lines in risk management, team incentives, and inherent in how attackers operate versus how defenders manage themselves.

76%

76 percent of respondents say that cybersecurity risk is now a top three risk factor.

83%

83 percent of respondents continue to report damage due to cybersecurity breaches.

54%

54% of the executives surveyed reported more concern over cybercrime than in the previous year.

More than 50% of respondents complain that no incentives exist for cybersecurity.

Ideas/money

Upper-tier cybercriminals steal ideas while lower-tier criminals steal money.

51%

Only 51% of polled IT specialists in Russia had found jobs in the legitimate IT sector.

42%

As many as 42 percent of vulnerabilities are exploited by criminals within 30 days of being disclosed.

5

Operators were five times more likely to report that no incentives exist for cybersecurity.

54%

54% of the executives surveyed reported more concern over cybercrime than in the previous year.

Less than 50% of organizations have fully implemented their strategies.

Less than half of organizations have fully implemented their strategies.

Limited effectiveness

Implementers fail to follow through, implement, or adapt their strategies.

5% more likely

Operators were five times more likely to report that no incentives exist for cybersecurity.

Lower barriers to entry

Drawing on a broader talent pool, including young people and foreign ICT experts that are often drawn into cybercrime, can help fill the cyber skills gap for companies and drain talent from the criminal market.

Use public disclosure

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.