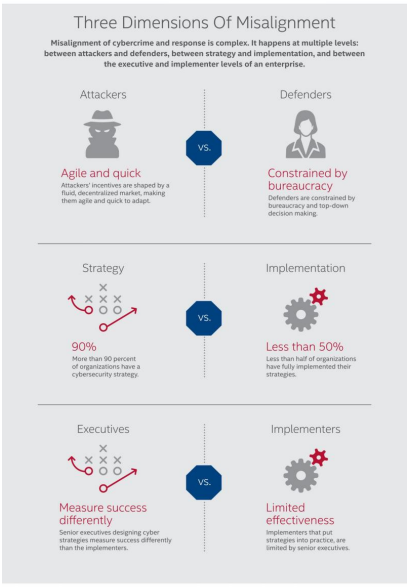
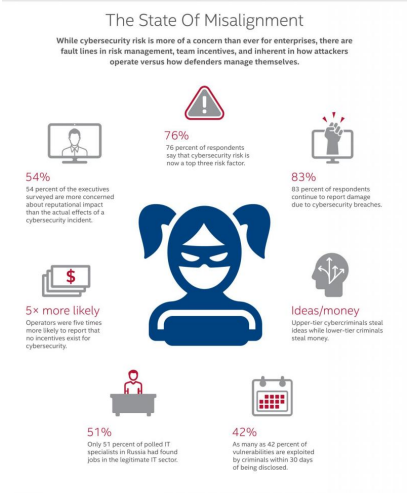
New global cybersecurity report reveals misaligned incentives, executive overconfidence create advantages for attacker

March 1 2017

Misaligned Incentives

Driven by market forces, cybercriminals are outpacing defenders.





Get aligned. Learn from attackers.
Adapt and thrive.

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

intel Security

Credit: Intel

Intel Security, in partnership with the Center for Strategic and International Studies (CSIS), today released "Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity," a global report and survey revealing three categories of misaligned incentives: corporate structures versus the free flow of criminal enterprises; strategy versus implementation; and senior executives versus those in implementation roles. The report highlights ways organizations can learn from cybercriminals to correct these misalignments.

Based on interviews and a global survey of 800 cybersecurity professionals from five industry sectors, the report outlines how cybercriminals have the advantage, thanks to the incentives for cybercrime creating a big business in a fluid and dynamic marketplace. Defenders on the other hand, often operate in bureaucratic hierarchies, making them hard-pressed to keep up.

Additional misalignments occur within defenders' organizations. For instance, while more than 90 percent of organizations report having a cybersecurity strategy, less than half have fully implemented them. Moreover, 83 percent say their organizations have been affected by cybersecurity breaches, indicating a disconnect between strategy and implementation.

And while cybercriminals have a direct incentive for their work, the survey not only shows there are few incentives for cybersecurity professionals, but that executives are much more confident than operational staff about the effectiveness of the existing incentives. For

example, 42 percent of cybersecurity implementers report that no incentives exist, compared to only 18 percent of decision-makers and eight percent of leaders.

"The cybercriminal market is primed for success by its very structure, which rapidly rewards innovation and promotes sharing of the best tools," said Candace Worley, vice president of enterprise solutions for Intel Security. "For IT and cyber professionals in government and business to compete with attackers, they need to be as nimble and agile as the criminals they seek to apprehend, and provide incentives that IT staff value."

"It's easy to come up with a strategy, but execution is tough," said Denise Zheng, director and senior fellow, technology policy program at CSIS. "How governments and companies address their misaligned incentives will dictate the effectiveness of their cybersecurity programs. It's not a matter of 'what' needs to be done, but rather determining 'why' it's not getting done, and 'how' to do it better."

Other key findings of the report include the following:

- Non-executives are three times more likely than executives to view shortfalls in funding and staffing as causing problems for the implementation of their cybersecurity strategy.
- Even though incentives for cybersecurity professionals are lacking, 65 percent are personally motivated to strengthen their organizations' cybersecurity.
- Ninety-five percent of organizations have experienced effects of cybersecurity breaches, including disruption of operations, loss of IP, harm to reputation and company brand, among other effects. But only 32 percent report experiencing revenue or profit loss, which could lead to a false sense of security.
- The government sector was the least likely to report having a

fully implemented cybersecurity strategy (38 percent). This sector also reports having a higher share of agencies with inadequate funding (58 percent) and staff (63 percent) than the private sector (33 percent and 43 percent, respectively).

The report also suggests ways the defender community can learn from the attacker communities. These include:

- Opting for security-as-a-service to counter cybercrime-as-a-service
- Using public disclosure
- Increasing transparency
- Lowering barriers to entry for the cyber talent pool
- Aligning performance incentives from senior leadership down to operators

The good news, according to the report's authors, is that most companies recognize the seriousness of the cybersecurity problem and are willing to address it. Organizations need more than tools to combat cyberattackers; experimentation is necessary to determine the right mix of metrics and incentives for each organization as they approach cybersecurity through more than just a cost-conscious framework and become more innovative in their organizational structure and processes.

Methodology

Intel commissioned independent technology market research specialist Vanson Bourne to undertake the research upon which this report is based. Intel surveyed more than 800 respondents from companies ranging in size from 500 employees to more than 5,000 across five major industry sectors, including finance, health care and the public sector. The survey targeted respondents with executive-level responsibility for cybersecurity as well as operators who have technical

and implementation responsibilities for cybersecurity. Countries represented by respondents include Australia, Brazil, France, Germany, Japan, Mexico, Singapore, United Kingdom and United States.

More information: For more information about these findings and to view the full report, visit www.mcafee.com/misaligned

Provided by Intel