Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity

Center for Strategic and International Studies
Contents

Cybersecurity Is Now a Top Priority  5
“A Tax That We All Don’t Want to Pay …”  8
A Disconnect Between Strategy and Implementation  9
Measuring Effectiveness  11
What Motivates Improvements in Security?  12
Searching for Solutions  17
The Black Hat Ecosystem  22
Specialization in the Criminal Market  23
The Cybercrime Market: Competitive, Decentralized, Innovative  24
Big Budgets Support Innovation in the Grey Market  26
Black Hat or White Hat?  27
Part-Time Crime is More Common in the Russian-Speaking World  29
Realigning Incentives to Strengthen Cybersecurity  31
Cybercriminals have the advantage. This has been true since the internet was commercialized 20 years ago. The incentives for cybercrime have made it a big business and a dynamic marketplace. Defenders are hard pressed to keep up.

Misaligned incentives explain much of this—both within organizations and between attackers and defenders in cyberspace. Misaligned incentives between attackers and defenders mean that the decentralized market in which cybercriminals operate makes them adapt and innovate faster and more efficiently than defenders, whose incentives are shaped by bureaucracies and top-down decision making.

Some of the advantage cybercriminals have over defenders is due to technology—we now all know that the internet was never designed to be secure. Some is due to policy. There are countries that tolerate, shelter, and maybe even encourage cybercrime. Governments and companies know they are at a disadvantage, but they are playing catch-up. Managing the risk posed by cyberthreats has become a priority, but the best criminals still seem able to stay ahead, even as companies allocate more resources to cybersecurity.¹ This does not mean cybercrime will always win. It does mean that companies and governments will need to rethink how they measure, reward and incentivize defense.

Markets send signals by creating prices and rewards, creating incentives for action. The cybercrime market is efficient, and the incentives for cybercriminals are clear and compelling. The same is not true for defenders. Criminals flourish in this market, but most defenders work in bureaucracies. In most companies, cybersecurity is the responsibility of a diverse range of groups and individuals using different (and sometimes conflicting) metrics for success.

Incentives are not only misaligned between attackers and defenders, but within companies. To examine this misalignment of incentives, we conducted a survey of 800 respondents from companies ranging in size from 500 employees to more than 5,000 across five major industry sectors, including finance, healthcare, and the public sector. Our survey targeted respondents with executive level responsibility for cybersecurity, as well as operators that have technical and implementation responsibilities for cybersecurity. The results provide insight into how each group views cyber risk in making decisions about an organization’s cyber-risk management strategy. Better calibrating the misaligned incentives we uncovered may yield a more coherent and effective cybersecurity posture for companies worldwide.

¹ SANS Institute, “IT Security Spending Trends,” February 2016
Our survey found three key misalignments in cybersecurity. Within organizations, incentives are misaligned between strategy and implementation and between senior executives and those with operational responsibility.² Most importantly, the governance processes, risk management policies, and structured workflows within cybersecurity are at odds with the freeform, ad hoc networking that is at the heart of adversary innovation. The top-down, corporate governance structures for defenders lies in stark contrast to the dynamic and free-flowing structure their adversaries occupy.

### Three levels of misaligned incentives put defenders at a disadvantage

<table>
<thead>
<tr>
<th>Attacker vs. Defenders</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy vs. Implementation</td>
<td>While more than 90% of organizations have a cybersecurity strategy, less than half have fully implemented their strategies.</td>
</tr>
<tr>
<td>Executives vs. Implementers</td>
<td>Senior executives designing cyber strategies measure success differently to those who put strategies into practice, limiting their effectiveness.</td>
</tr>
</tbody>
</table>

Senior company executives develop strategies to reduce cyber-risk and mitigate the potential effects on critical activities in their enterprise. Operators and IT managers are then responsible for identifying and deploying a mix of practices and technologies to implement these strategies. Our study found that there is a misalignment of incentives between executives and operators regarding their respective approaches to managing cyber-risk.

For attackers in cyberspace, or “black hats,” the risks and rewards are much more clear. Black hats, a term taken from spaghetti westerns, means any hackers that break into systems without the owner’s permission, whether they are governments conducting espionage, criminals out for financial gain, or hacktivists motivated by ideology. Black hats are part of an underground ecosystem that channels tools, expertise, and infrastructure into criminal operations that extract billions of dollars of profit from data theft, extortion, and fraud. This ecosystem is largely comprised of commoditized markets of specialized freelancers with different skills and expertise. This loose, informal structure provides low barriers to entry, transparency and competition, and efficient allocation of resources that allows black hats to tap a wide talent pool, innovate quickly, and adapt quickly to changes in defenses and technology.

² Executives include respondents who identified as company owner, director, CEO, CIO, CISO, CTO, or CISO, and operators include those who identified as head of IT or data protection, IT department manager, or IT team leader.
The incentive structure for black hats in the cybercrime market drives attackers toward rapid collaboration, innovation, and specialization that make it a relatively efficient and flexible marketplace. The black hat community draws from a large talent pool and relies on a freelance model to produce highly specialized products and exploits for specific attack purposes. This market is also more efficient and fluid, being able to adapt quickly and with more ease based on an attacker’s motives. This underground economy creates an entirely different, powerful set of incentives for attackers to succeed and stay atop of the market.

The black hat ecosystem is comprised of two markets: a high-tier market of highly sophisticated and well-resourced actors looking to exploit specific targets with highly advanced techniques, and a low-tier market comprised of criminals and hacktivists launching opportunistic attacks on any vulnerable systems they can find.³ These markets have some overlap, and many of the tools initially trafficked in the high-tier market eventually trickle down to the low-tier market as they age and become more widely known.⁴

Cybersecurity Is Now a Top Priority

Internet users have been slow to react to the black hat advantage. Six years ago, cybersecurity did not even rank in the top 10 risks prioritized by company boards.⁵ There was little understanding of how cybersecurity fit into risk management. Many company boards did not allocate resources to practices now thought of as fundamental, such as conducting security program assessments, assigning responsibilities to privacy and security roles, and receiving regular reports on cybersecurity risks.

Hard lessons have been learned since then as companies and governments around the world have experienced cyberattacks exceeding $400 billion in total annual cost. A majority of respondents to our survey now rate cybersecurity risk as one of the top three risks facing their organization, confirming that cybersecurity now ranks among the top concerns for companies.⁶

Our survey shows a marked change in board attitudes toward cybersecurity. A majority of respondents reporting both that their boards understand and prioritize cyber-risk. Furthermore, nearly three-quarters (72%) of respondents indicated that their company boards are being briefed on cybersecurity risks at most or every meeting.

A majority of respondents rated cybersecurity risk as one of the top three risks facing their organization.

⁵ Lloyds, “Lloyd’s Risk Index,” 2011
Respondents in all sectors see a significant cyber threat to critical aspects of their organization, ranking the loss of intellectual property and confidential business information, disruption of operations, and harm to company reputation and brand as the largest risks that could result from poor cybersecurity practices.
The observed effects of a cybersecurity incident experienced by survey participants largely mirror the perceived risks from above. More than four in five (83%) respondents report that their organizations have seen an effect as a result of cybersecurity breaches, with the disruption of operations, loss of intellectual property, and harm to company reputation or brand once again ranking among the top areas affected.
“A Tax That We All Don’t Want to Pay …”

Despite the overwhelming response from survey respondents that cyberbreaches have resulted in disruptions, IP loss, and harm to company reputation, less than a third (32%) reported experiencing revenue or profit loss as a result of a cybersecurity incident. The perception that cyberbreaches do not directly lead to loss of revenue or profit may be giving companies a false sense of security.

It is also interesting to look at differences in opinion between individuals at the executive level versus those who serve in technical and operational roles. Our study shows that executives view breaches as a cost of doing business. Sixty-three percent of executives say as much, while operators that work for them focus on reducing the number and scope of breaches. For executives, cybersecurity competes with a range of other company imperatives, some of which are in direct conflict with investing in security. Executives from one large company called cybersecurity “a tax that we all don’t want to pay …” \(^8\)

Organizations may also lack the metrics to assess indirect costs as the result of a breach, such as quantifying the time spent notifying customers, damage to brand loyalty, or time spent investigating an incident. Incomplete data on cost could mean that executives have an inflated level of tolerance for poor cybersecurity. In fact, more than a majority (54%) of executive respondents say that their organizations are more concerned about reputation than cybersecurity itself.

---

7  “Business warned not to be complacent about cyber security,” Computer Weekly, September 20, 2016
A Disconnect Between Strategy and Implementation

Companies and governments across all the sectors and regions we surveyed are developing cybersecurity strategies at a rapid pace. More than nine in ten (93%) of respondents said that their organizations now have a cybersecurity strategy designed to combat both existing and new threats.

Executives may be overconfident in their organization’s ability to manage emerging threats. Operators, who are on the front lines of cyberdefense, tend to believe that their organization’s cybersecurity strategy is less forward looking, focusing more on current rather than emerging threats.

Cybersecurity strategy design balance

Executives versus operators and sector respondents on how much their organization’s cybersecurity strategy is designed to manage existing versus new threats.
Differences across sectors are also worth noting, as the finance and IT/telecom sectors have a more balanced approach to managing current and future threats. In contrast, the cybersecurity strategies of public sector organizations, including government and educational institutions, are less forward looking and skew toward managing existing threats rather than future threats. Given that most government and public sector organizations are not well regarded for their cybersecurity know-how, this is not unexpected.⁹

Although respondents overwhelmingly report having a cybersecurity strategy, implementation remains a major challenge, as less than half of respondents (49%) report that their cybersecurity strategy is fully implemented across their organization. Our study also found that executives and operators disagree on the extent to which their cybersecurity strategy is actually implemented, as well as on the metrics used to evaluate the level of implementation.

Executives tend to view their organization’s cybersecurity strategies as more fully implemented than operators. They are also more likely to evaluate the effectiveness of their cybersecurity strategies through the lens of broader organizational goals, including cost control and maintaining reputation, than operators who focus more on technical cybersecurity metrics.

---

*There are assumptions we made and assessments of the nature of the threat that in retrospect weren’t sufficient.*

—Frank Blake, CEO, Home Depot¹⁰

---

9 CSIS, The Role of Shared Services and the Cloud in Enhancing Cybersecurity, Cyber Policy Task Force Working Group Discussion Papers, 2016

Measuring Effectiveness

The disconnect between strategy and implementation is partly due to the fact that those who determine the strategy (executives) and those who implement the strategy (operators) are not measuring effectiveness and outcomes using the same set of metrics.

In general, operators looked to metrics such as breach numbers, penetration testing, vulnerability scans, and cost-of-recovery analysis to measure their organization’s cybersecurity effectiveness. However, executives are more likely to rely on general performance and cost-centric metrics to gauge their cybersecurity strategy effectiveness.

Both executives and operators rank the overall number of breaches as the preferred metric to gauge their cybersecurity strategy’s effectiveness. Executives, however, are more likely to focus on the cost of recovery from a breach, negative publicity, or the number of employed cybersecurity staff.
Executive respondents also ranked “proprietary metrics to gauge return on investment for cybersecurity spending” significantly higher than operators when measuring the effectiveness of their organization’s cybersecurity strategy. While metrics are essential to establishing qualitative criteria in order to evaluate effectiveness for any risk management strategy, there is not yet a consensus on whether the use of “return on investment” (ROI) provides for accurate, risk-based cybersecurity evaluations.¹¹ By comparison, operators ranked technical metrics higher than executive respondents, with vulnerability scans ranking second and penetration testing third among ways they measure their organization’s cybersecurity strategy.

What Motivates Improvements in Security?

Incentives shape how people and organizations behave. Our survey shows that cybersecurity professionals lack adequate incentives. Most respondents report that, while some incentives do exist, they are lacking for cybersecurity professionals. Executive participants in our survey were more confident than operators about the existing incentives for cybersecurity professionals, indicating they are more likely to believe all categories of incentives are available to security professionals in their organization.

---

Operators were five times more likely to report that no incentives exist for cybersecurity professionals in their organization. Almost half of operators reported no incentives existing in their organization. It is possible that incentives, even when they exist, may not actually be known by employees, especially if they are lower down in the organization’s structure.

**Existing incentives for cybersecurity professionals**

Executives versus non-executive respondents on incentives that exist for cybersecurity professionals

Although our survey results show that many respondents believed incentives for cybersecurity professionals are lacking, 65% of respondents said they were "personally motivated" to strengthen their organization’s cybersecurity. The first result (incentives are lacking) is probably more accurate. Responses relating to organizational success, such as preventing data breaches, defeating hackers, reducing the risk of organizational reputational damage, and financial impact, were ranked higher by respondents than were categories relating to personal success, such as harm to personal reputation or job security. These results may reflect respondent bias, with participants self-reporting on putting the success of their organization ahead of their own interests.
So what’s the real story? Individuals responsible for cybersecurity define success differently, and are motivated by a mix of performance incentives. Both executives and operators value financial compensation and recognition or awards the highest over paid time off and promotions. However, our study showed that operators are almost equally motivated by recognition and awards as they are by financial compensation. An earlier study on how organizations attract and retain skilled security professionals found that having employers paying for training, allowing for flexible schedules, and providing opportunities to engage in challenging tasks were valued more highly than compensation by security professionals when looking at possible employers.¹² In contrast, executives ranked financial compensation significantly higher than any other form of incentive.

---

Respondents in different countries displayed a range of views on incentives perhaps due to differences in cultural norms. Japan and the United Kingdom valued recognition or awards higher than other incentives, while Mexico and Germany valued them the least. Respondents in Brazil, Mexico, and the United States were most likely to place the most value in financial compensation. Japan, Mexico, and Germany put a higher premium on paid time off than other countries in our survey.
Incentives cybersecurity professionals would like more of

- Financial compensation
- Recognition or awards
- Promotion
- Paid time off

Executive vs. Operator

Incentives country respondents would like more of

- Brazil
- Mexico
- US
- Germany
- France
- UK
- Japan

Financial compensation (bonus)
Recognition or awards
Promotion
Paid time off
Searching for Solutions

As organizations learn to manage risk and adapt to new cyberthreats, they appear to be eager to work with the government. A majority of respondents in most sectors share threat intelligence with partner organizations, as well as with the government and outside consultants.

A significant majority of respondent organizations view voluntary models of collaboration with the government as valuable in helping to create cybersecurity incentives within organizations. Executives appear to value public-private partnerships more than operators, suggesting these models could be better structured to benefit IT operators in order to provide value to their day-to-day technical mission.

Organizations value public-private partnerships

Organizations on whether voluntary models create useful incentives for cybersecurity

Companies see cooperation with government as an important part of their cybersecurity strategy and a key means of improving their cybersecurity. But less than half of respondent organizations report using unclassified government briefings as a source of information when making decisions about cybersecurity. More than three-quarters of organizations believe that faster access to security clearances would be the most effective way to improve their cybersecurity posture, and 66% want greater access to government threat intelligence.
This may be a case of do what we say, not what we do. Companies appear to be motivated and incentivized to work with the government with the expectation of gaining access to information to improve cybersecurity.

Companies value interactions with the government as a source of information, but in many cases, we found that the government sector performed lowest in areas of cybersecurity competency when compared with other surveyed sectors. Based on the survey, government sector entities appear to be locked into a reactive cybersecurity model skewed toward managing existing threats versus new ones. They were also the least likely to report having a fully implemented cybersecurity strategy or provide incentives to cybersecurity professionals.
By country, respondents to our survey in the United States, Brazil, and Germany place the most value in public-private partnerships. Mexico, Brazil, Germany, and the United States all would like faster access to security clearances, while the United Kingdom ranked having access to government threat information higher than access to security clearances. Across the board, countries ranked using government briefings as a source of information to make cybersecurity decisions either third or fourth in importance.
In a previous report, “Hacking the Skills Shortage,” we found that nine out of 10 respondents believe technological advancements could compensate for the cybersecurity skills shortage.¹³ This confidence was not reflected in this survey, where respondents ranked third-party managed services and leveraging automated workflows to manage lower level threats fourth and fifth respectively in ways to ensure new cyberdefense measures don’t open them up to new risk. The findings of this report suggest that the evolving threat landscape will not only change the demand for a skilled cybersecurity workforce, but also for new and innovative tools and practices.

Innovation in the cybersecurity space can be complicated as new cyberdefense technologies require extensive vetting in order to ensure they do not have vulnerabilities that expose users to additional risk. In recent interviews with senior cybersecurity, technology and risk management specialists from across the financial services industry, it was found that CISOs often have difficulty assessing and integrating new security tools due to the rapid pace at which they are developed and released, all the while attempting to better align their cybersecurity policies with the business, operational, and technology strategies of their companies.¹⁴


In a 2015 survey on risk and innovation, a significant majority of respondents said that their organization had invested in security technology that was "ultimately discontinued or scrapped" soon after being deployed.\textsuperscript{15} The shortages in skilled cybersecurity workforce and in-house expertise further compounds the difficulty organizations have in producing innovative approaches to cybersecurity.

To avoid new risk exposure, most respondent organizations to our survey maintain a security platform that integrates existing and new technologies, or acquire overlapping security technologies. Over half of organizations viewed investing in more talent to manage cybersecurity events as a way to ensure cyber defense measures do not result in new risk.\textsuperscript{16}

\begin{quote}
“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”
—Bruce Schneier\textsuperscript{17}
\end{quote}


\begin{figure}
\centering
\includegraphics[width=\textwidth]{practices_bar_chart.png}
\caption{Practices used to limit risk when using new cyberdefense tools}
\end{figure}
The Black Hat Ecosystem

In contrast, the “black hats” against whom companies must defend lack neither workforce nor innovative technology. The black hats have clearly designed incentives created by market forces, not by organizational fiat. The market economy of the criminal hacker ecosystem facilitates innovation and rapid adaptation, and channels resources efficiently to the lowest cost and most profitable criminal enterprises. Unlike the defensive market, in which the strictures of corporate hierarchy affect priority setting and decision making to create a slow, bureaucratic process (even in the best of companies), the criminal market is competitive, commoditized and decentralized.

This open and decentralized criminal market creates strong incentives for criminals to strive to be the best, attracting the largest customer base and commanding premium prices. With low barriers to entry for new products and services, criminals have to remain innovative and maintain a strong reputation to stay at the top of the market. Unsurprisingly, we were unable to survey members of the black hat community, relying instead on interviews with technical experts, police and cybersecurity experts. Their experience and observations identify a fast-paced, well-resourced, and dynamic cybercrime ecosystem where incentives are clearly aligned with objectives.

The top tier of the black market is comprised almost exclusively of elite technical specialists selling highly coveted zero-day vulnerabilities, intermediaries who specialize in high-dollar-value exploits that serve as brokers between buyers and sellers, and governments that buy tools in the white or grey market for everything from domestic surveillance to cyberespionage.¹⁸ The grey market includes many black hats but few criminals—while they access systems surreptitiously, most grey market participants claim they work exclusively with governments who can pay top dollar, and they avoid the risk of arrest and of dealing with criminals and scammers in the low-tier market.¹⁹ Zero-days and highly sophisticated tools are almost exclusively sold in this market for the same reason.

The lower tier, dominated by criminals and the networks that support them, is made up primarily of products like financial information and counterfeit goods, as well as “exploit-as-a-service” and spamming services, as opposed to sophisticated tools and exploit kits, which are primarily in the upper tiers.²⁰ Exploit kits and crimeware services offered in the lower-tier market often take advantage of older, unpatched systems or vulnerabilities that have not been addressed by vendors, as opposed to expensive zero-day vulnerabilities.²¹ While upper-tier actors commit espionage, steal intellectual property (IP), and launch destructive attacks, the lower-tier criminals are driven primarily by money.²²

---

Specialization in the Criminal Market

Virtually anyone who is computer literate can participate in the criminal market.²³ This criminal market is made up of a network of specialists, ranging from providers of compromised hosts and human services to exploit kits and compromised accounts, supporting a wide variety of criminal businesses or strategies to monetize these tools and services through spam, fraud, data theft, and extortion.²⁴

Each of these actors has their own specialized profession, which either enables others further down the chain to acquire money from victims, or provides incentives for actors further up the chain to develop new tools and services. The most common specialties/professions in these chains are:²⁵

- Programmers—who develop malware.
- Web designers—who create malicious sites.
- Tech experts—who maintain the criminal infrastructure (servers, databases).
- Hackers—who exploit system vulnerabilities and break into computer networks.
- Fraudsters—the classic con artists who devise social engineering schemes (phishing, spam).
- Intermediaries—in general, these are criminals who collect data stolen from users, advertise it to other cybercriminals, sell, or exchange it for money or other illegal actions.

²³ Ablon, Libicki, and Golay. Ibid.
Profits from criminal businesses are then divvied up among these specialists. According to one law enforcement expert, 80% to 90% of proceeds typically go to the supporting technical specialists and money mules, not to the criminals that devise the schemes.

**The Cybercrime Market: Competitive, Decentralized, Innovative**

The cybercriminal market is dynamic and 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. For example, one expert we interviewed reported that after version 3.0 of the CryptoWall malware family was disrupted, its developers were able to release version 4.0 within days. Similarly, when the developers of the once-dominant Angler exploit kit (which made up 82% of exploit kit activity, according to one estimate) were arrested,²⁶ within weeks attackers who had relied on Angler adopted the Neutrino exploit kit to replace it and deliver their payloads.²⁷

The fast pace of innovation in the criminal market is the result of a combination of factors. First and foremost, criminals are opportunistic, and the free availability of support services in the black market makes them nimble and quick to act, putting defenders at a disadvantage.

For example, when new vulnerabilities and exploits are disclosed, criminals quickly find ways to exploit them for profit. One study found that 42% of disclosed vulnerabilities are exploited by criminals within 30 days of disclosure,²⁸ meaning that as these vulnerabilities are disclosed publicly, the criminal underground quickly adopts them into new attacks. Criminals are also opportunistic and focus their energies on the lowest-hanging fruit. Instead of investing in costly vulnerability research and exploit development, they take advantage of publicly disclosed vulnerabilities to exploit unpatched systems.

Leveraging publicly disclosed vulnerabilities and exploits in their attacks eliminates the costliest and most time-consuming part of the development cycle—vulnerability research and exploit development. Most of the exploit kits offered on the criminal market use known vulnerabilities, and some of our experts even reported that criminals have taken to advertising the CVE numbers of the vulnerabilities used in their products. While costly capability development is supported by million dollar contracts in the upper-tier market, the lower-tier market is sustained at much lower prices by the free availability of publicly disclosed vulnerabilities and the plethora of unpatched systems that can be exploited in the aftermath of disclosure.

"For cybercriminals, unpatched vulnerabilities in popular software, such as Microsoft Office or Adobe Flash, represent a free pass to any target."

---


In a competitive and open market, success requires being the best

Cybercrime is a competitive market founded on reputation and thorough product vetting, so developing new capabilities or providing superior service is paramount for cybercriminals to outdo their competitors. The open and competitive nature of the market creates a strong incentive to be the best. As one expert we interviewed put it, “Attacker don’t innovate for the sake of innovating,” they do it to maintain competitive advantage or exploit newer and more lucrative opportunities.

In the underground, “good products squeeze out bad ones, and high-quality brands can command premium prices ... new products thrive or wither depending on the judgment of the market.”²⁹ As criminals develop new schemes, they are tested by the market, and while those that succeed can quickly scale up their resources and support by buying services in the open market, those that fail quickly disappear and their developers turn to new projects.

In order to succeed in this fast-paced and competitive marketplace, criminals must constantly strive to be better than the competition, creating a race to the top that supports the most innovative and efficient operators.

Innovation is not limited to new malware. Sometimes, criminals can find profit in novel marketing schemes or repackaged goods. Threat intelligence company SecureWorks observed Russian hackers offering free five- to 10-minute “tests” of their DDoS service before proceeding with the lease transaction.³⁰ Skilled underground players are also making money off of lower-skilled cybercriminals, offering malware-as-a-service, social engineering tutorials, and carding (stealing credit card information) “bibles,” or guides for would-be criminals.

---


The relative transparency of the criminal underground, where many attackers participate in shared forums and love to brag about their successes, helps these innovations to proliferate and achieve scale quickly. When one criminal sees that customers are attracted to a new service offered by a competitor (24/7 customer support, pre-purchase tests or demos of the product, working through guarantors that ensure both parties do not get ripped off), they quickly adopt the same practices in order to remain competitive.

Similarly, attackers swarm around targets and attack methods that prove lucrative for their competitors. For example, after some enterprising attackers began making significant profits from ransomware attacks on hospitals in 2015, recognizing that they could not afford to let their systems go down with patients’ lives on the line, other operators quickly followed suit. The ransomware community swarmed around these soft targets so intensely that by mid-2016, one report found that 88% of detected ransomware attacks were targeting healthcare companies.³¹

**Big Budgets Support Innovation in the Grey Market**

Companies in the more exclusive “grey” markets are quick to replace and repurpose capabilities because their customers demand it. Catering primarily to governments and major corporations whose primary purpose is surveillance and intelligence gathering, they often maintain a backlog of vulnerabilities and exploits that they use to replace capabilities that are burned. In some cases, customers want multiple exploits available for the same systems so that they can vary their attack methodology, reducing the probability of detection and attribution. Others want to ensure that there are no breaks in their intelligence coverage, meaning they want new tools to be available as soon as old ones are burned.

These customers have massive budgets, and are willing to pay top dollar—in some cases hundreds of thousands of dollars or more³²—for these capabilities, allowing companies to invest the time and money necessary to develop and maintain a backlog of elite tools. They can also afford to vacuum up any zero-days discovered by other hackers, whether amateurs, white hats, or criminals. While data on the price of zero-day malware and exploits is hard to come by, intermediaries like Zerodium are willing to pay extremely high prices for exclusive access to these tools.

---


researchers moonlighting in their off hours, former government hackers, or out-criminals. While some are self-taught, others are IT professionals or security “script kiddies,” today’s underground economy is dominated by professional hat hackers were students and young people fascinated by computers, so-called or cybersecurity industries or pursuing a criminal career. While many early black Attackers and defenders in cyberspace often have similar skills and backgrounds. Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Black Hat or White Hat?

Attackers and defenders in cyberspace often have similar skills and backgrounds. People with technical skills face a choice between going into the legitimate ICT or cybersecurity industries or pursuing a criminal career. While many early black hat hackers were students and young people fascinated by computers, so-called "script kiddies," today’s underground economy is dominated by professional criminals. While some are self-taught, others are IT professionals or security researchers moonlighting in their off hours, former government hackers, or out-of-work computer science graduates.

Prices offered for zero-day tools by grey market intermediary

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Black Hat or White Hat?

Attackers and defenders in cyberspace often have similar skills and backgrounds. People with technical skills face a choice between going into the legitimate ICT or cybersecurity industries or pursuing a criminal career. While many early black hat hackers were students and young people fascinated by computers, so-called "script kiddies," today’s underground economy is dominated by professional criminals. While some are self-taught, others are IT professionals or security researchers moonlighting in their off hours, former government hackers, or out-of-work computer science graduates.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defenders.

Grey market firms can also repurpose capabilities. While many of these companies focus on providing offensive capabilities for surveillance and intelligence gathering, they also offer fuzzing services, penetration testing, and white hat security services. When a zero-day used in offensive operations is burned, it may be incorporated into a penetration testing tool or used to develop indicators of compromise that can be marketed to defendants.
Many old school black hats have moved into the legitimate cybersecurity industry as opportunities have grown and law enforcement has cracked down on cybercrime. These early hackers, many of whom got involved in black hatting to learn about cool exploits and make a name for themselves, were eventually drawn to bigger and better-paying opportunities in the defense market. As one former black hat we interviewed said, “I crossed over to get access to new and cooler tech and bigger environments … I got to hack super-cool systems as a white hat!”

Highly skilled programmers and vulnerability researchers primarily work in top-tier white and grey markets. With access to six-figure salaries at legitimate companies, no fear of arrest, and the opportunity to spend their time figuring out how to hack the most complex and “cool” systems, there is little incentive to be involved in criminal activity. This is especially true for the most elite hackers that find and exploit zero-day vulnerabilities. One user summed up the choice facing hackers who identify zero-days clearly in an online hacker forum:

"Almost no reason to sell zero-days on the black market anymore if you can broker it to security firms. Risk is high and chance of being ripped off is crazy high when selling on black market. Another plus being that zero-day sold to reputable security firms can land you a six-figure job."³³

A criminal background can also make it difficult to get into the white and grey markets. Grey and white market companies rely on reputation and connections to secure lucrative contracts with governments and major corporations. These contracts often involve administrator access to highly sensitive or classified data and systems, and most customers are wary of allowing criminals or former criminals high level access to their systems.

There are exceptions, however. For example, a student at Carnegie Mellon University was arrested in 2015 for creating and disseminating the “Dendroid” malware family, which compromised Android apps and allowed attackers to gain complete control of Android devices.³⁴ He sold the malware on Dark0de, the top English language cybercrime forum,³⁵ to any interested customer for $300 and even offered 24/7 customer support.³⁶

---


Part-Time Crime is More Common in the Russian-Speaking World

While highly skilled hackers rarely participate in criminal activity in the West, in some regions there is more overlap between the white/grey markets and the criminal market. In particular, the Russian-speaking hacker community is highly fluid, is home to many of the world's most sophisticated cybercriminals, and involves a higher degree of overlap between the legitimate ICT and cybersecurity industries and the criminal ecosystem.

One expert interviewed for this report noted that many of the top Russian-speaking hackers that he identified work for legitimate ICT companies while moonlighting as criminals. The majority of these are Russian or Eastern European IT and telecom companies, but some work for legitimate cybersecurity companies. Some of these criminals even list their criminal identities and dark web handles on their open Facebook pages, right next to their legitimate day job.

Some of the most sophisticated Russian cybercriminals are also plucked from Russia's advanced math and computer science programs and trained by the intelligence services. One expert we talked to described Russia's approach to hacking as similar to their approach to Olympic athletes. The government invests significant resources in developing an elite athlete who competes for the nation, then they go independent and make millions playing for themselves.

Some experts argue that this greater overlap with the legitimate ICT industry is the result of a permissive environment for transnational cybercrime. There is a well-known rule in the Russian underground that you do not hack Russians or Russian-speakers. According to law enforcement sources, Russian and Eastern European authorities are tolerant of cybercrime as long as the targets are in Western Europe, the US, or Asia, but can be quick to take action against criminals that target computers in their jurisdiction.

As one law enforcement official told us, some of the major prosecutions of Russian and Eastern European cybercriminals by US law enforcement have started with a call from the FSB—"We've identified a cybercriminal who is responsible for serious crimes in your country. We would be happy to cooperate with you in bringing them to justice." Of course, in many cases, these criminals have been operating openly in their home country for years, and the FSB only "identified" them after they made the mistake of using their skills against targets in Russia.

Criminals know this, and use a variety of techniques to constrain their attacks to foreign computers. For example, the Citadel Botnet included an interesting quirk in the malware—it only infected computers using the Roman alphabet, but did not infect computers whose operating systems are in Cyrillic, ensuring that Russian and Ukrainian authorities would take little interest.³⁸ As shown in the heat map below, the botnet was prolific in western Europe and the US, but infected very few computers in the Russian-speaking world. A cluster of infections in Moscow reflected the concentration of foreigners living in the Russian capital.

The shortage of legitimate ICT jobs in Russian and Eastern Europe also pushes many talented ICT experts into criminal activity. Many hackers in the Russian criminal underground are out-of-work IT experts and computer science graduates who are unable to find legitimate jobs. A 2013 survey by recruiting website HeadHunter found that only 51% of polled IT specialists in Russia had found jobs in the legitimate IT sector. Given their abilities, honed in top-tier technical universities, weak law enforcement, and the low wages even for those that do make it: “People think: why not earn a bit on the side?”⁴⁰

Breaking down the geographic and institutional barriers with the Russian-speaking cybercommunity can help to channel more of the talent and resources in that region into the legitimate cybersecurity industry. Russian universities produce highly talented programmers and mathematicians, but the lack of cybersecurity and ICT jobs in the Russian-speaking world and the lack of consequences for criminal activity push many of these professionals into criminal activity.

In contrast, the US and Europe face a shortage of talent in the legitimate ICT and cybersecurity industries, and computer science skills are highly marketable.⁴¹ With legitimate firms paying top dollar for security professionals, there is little incentive for skilled programmers to get involved in criminal activity. Tapping into the underemployed talent pool in Russia and Eastern Europe could not only help fill the skills shortage, but also shrink the talent pool supporting some of the most sophisticated cybercriminal operations.

---


⁴⁰ Ibid

For people with technical skills, high-paying job opportunities, low risk of arrest, and the opportunity to work with the top professionals and most cutting edge technologies create powerful incentives against participating in cybercrime. These incentives are distributed unevenly around the world, however. In the absence of legitimate opportunities and clear consequences for criminal behavior, as in Russia and Eastern Europe, the allure of making money and making a name for yourself can draw talented operators into cybercrime.

Realigning Incentives to Strengthen Cybersecurity

The scope and nature of the cybersecurity challenge is so complex and daunting that multiple measures at the international, national and company level are required to address it. This report looks at one segment of the problem—the governance issues that put companies at a disadvantage compared to their attackers.

The report identifies several critical areas on the defender side where divided attitudes, often split between technical and non-technical roles, toward organizations’ cybersecurity appear. These attitudes, such as how a cybersecurity strategy is designed, the degree of implementation, and its overall effectiveness, are central to how individuals develop an impression of their organization’s overall cybersecurity posture. The resulting differences in perception create an inaccurate, disjointed picture of a defender’s posture, undermining the goal of establishing an effective cybersecurity strategy and adding to the disadvantage defenders are at against black hat attackers.

The good news is that most companies recognize the seriousness of the cybersecurity problem and are willing to address it. We focus on governance, the processes, rules, and structure companies use to manage, make decisions on resources and technology, and compete—because these processes will usually be slower and less nimble than the market forces that drive attackers. This is in some ways inevitable, but it can be minimized through organizational innovation. Each company will need to identify innovation that best fits its business model and structure.

The tendency of executives to approach cybersecurity through a cost-conscious framework is no surprise. However, differences in how executives and operators measure risk and the misalignment of incentives is leading to suboptimal security. The establishment of a common set of metrics used by both executives and operators that took both cost and effectiveness into account would allow for a more coherent approach to companies’ cybersecurity efforts to mitigating risk.
Learning from cybercrime

Defenders can learn from the black hat community. “Security-as-a-service” can offer greater flexibility to counter the “crime-as-a-service” model of the criminal market, leveraging market forces to foster competition and strengthen incentives for defenders. The most effective defense (at companies that can afford it) blends in-house efforts and outside services and technologies.

<table>
<thead>
<tr>
<th>Lessons from the criminal market</th>
<th>Criminal market</th>
<th>Defenders’ analogue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leverage market forces</td>
<td><strong>Crime-as-a-service</strong>&lt;br&gt;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.</td>
<td><strong>Security-as-a-service</strong>&lt;br&gt;Greater use of outsourcing and open contracting can help reduce costs, increase competition, and facilitate the broad adoption of effective security technologies and practices.</td>
</tr>
<tr>
<td>Use public disclosure</td>
<td><strong>Target publicly disclosed vulnerabilities</strong>&lt;br&gt;Exploiting disclosed vulnerabilities avoids costly vulnerability research and exploit development, and quickly incorporates new disclosures into attacks to maximize value before defenders patch.</td>
<td><strong>Improve patching practices</strong>&lt;br&gt;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.</td>
</tr>
<tr>
<td>Increase transparency</td>
<td><strong>Open forums and online advertising</strong>&lt;br&gt;Open forums and public advertising facilitate the proliferation of successful new attacks and criminal business models and the widespread adoption of best practices.</td>
<td><strong>Information sharing and collaboration</strong>&lt;br&gt;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.</td>
</tr>
<tr>
<td>Lower barriers to entry</td>
<td><strong>“Anyone who is computer literate”</strong>&lt;br&gt;Lacking formal qualifications or geographical constraints, the criminal ecosystem is able to bring in undervalued talent from the legitimate economy and maximize its value.</td>
<td><strong>Tap global talent pool</strong>&lt;br&gt;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.</td>
</tr>
<tr>
<td>Align incentives</td>
<td><strong>Freelance markets reward performance</strong>&lt;br&gt;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.</td>
<td><strong>Performance incentives</strong>&lt;br&gt;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.</td>
</tr>
</tbody>
</table>
Attackers respond quickly to public disclosure of vulnerabilities, and leverage the transparency of online forums to spread best practices and new attacks. Defenders must accelerate efforts to patch vulnerabilities and replace legacy systems to match the speed of cybercrime. A faster patch and refresh cycle can raise costs to attackers, forcing them to invest in expensive and time-consuming vulnerability research and exploit development or go after other targets that are slower to raise their defenses.

Our research showed that black hats benefit from greater speed and focus. They are incentivized by direct rewards for being faster, newer, and nimbler in their attacks. The incentives for speed and focus are not there for defenders. But incentives can be changed. Companies have successfully experimented with their business models and structure to become more dynamic and innovative in order to remain competitive. The same sort of experimentation is necessary if cybersecurity is to keep up with the attackers. This will require identifying the right metrics for success and revamping organization structure to build a nimbler, faster defense. In thinking about how to do this, the best approach may be to take lessons from the black hats on how to create effective incentives.
About CSIS

For 50 years, the Center for Strategic and International Studies (CSIS) has developed practical solutions to the world's greatest challenges. As we celebrate this milestone, CSIS scholars continue to provide strategic insights and bipartisan policy solutions to help decision makers chart a course toward a better world.

CSIS is a bipartisan, nonprofit organization headquartered in Washington, DC. Its 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change.

http://csis.org/

About Intel Security

Intel Security, with its McAfee product line, is dedicated to making the digital world safer and more secure for everyone. www.intelsecurity.com. Intel Security is a division of Intel.