THE AMERICAN FOREIGN POLICY COUNCIL
Defense Technology Program Brief

June 2015 | Washington, D.C. | No. 11

Cyber Crime: Security Under Scarce Resources

By Trey Herr and Sasha Romanosky

Briefing Highlights

The relative security posture across firms and the cost of acquiring and implementing malicious software (i.e., malware) can influence target selection by these criminals. Successful cyber attacks can therefore be considered a result of mismatched investment in information security.

• • •

To combat cyber crime, one approach may be to attack the reputation mechanisms [user review systems within the cyber black market], disrupting the tenuous chains of trust that link buyers and sellers for malicious software and stolen information.

• • •

The data collected by insurance carriers affords them a unique advantage over any other entity—even government agencies—when it comes to assessing the benefits of different information assurance controls and practices.

• • •

Discussions regarding policies or regulations to force firms to increase cyber security should also be balanced with discussions of inducing *consumers* to take appropriate security and privacy precautions.

• • •

Framing information security as an investment proposes that the purpose of government intervention is to support a market that encourages companies to find the optimal point between the cost of attacks and benefit of defensive information assurance measures.

Cyber crime covers a wide range of activities that includes theft, fraud and harassment; stealing valuable intellectual property as part of industrial espionage; committing financial fraud and credit card theft; and disrupting internet services for ideological goals ("hacktivism"). The crimes target both firms and consumers, and while they rarely result in physical harm or property damage,[1] there can still be severe consequences.

For example, many data breaches are caused by criminals hacking into private corporations and government agencies in order to steal personal information. The compromised data may include individuals' names, addresses, social security numbers, dates of birth, driver's licenses, passport numbers, credit card numbers and other financial data. The information can then be used to commit crimes including unemployment fraud,[2] tax fraud,[3] loan fraud,[4] and payment card fraud. Individual harms stemming from these breaches include direct financial loss, the burden of increased loan interest rates, denial of utility services, civil suits or even criminal investigations.[5] The resulting costs incurred by firms might include forensic investigations, consumer redress, disclosure fees, and litigation—and sums can reach more than $200 million dollars.[6]

Overall, we frame this complicated topic as a discussion of two markets: one of information security, occupied by victims (e.g., firms and consumers), and one of threats, where buyers and sellers of malicious software and stolen information trade their goods.[7]

Policy solutions that attempt to reduce victim harms and cyber crime address more than just laptop and cellphone security. They seek to influence the incentives and behaviors of illicit actors and victims through criminal, civil, and administrative law, as well as regulation. The motivating question is: how can government interventions affect the incentives of actors in each

Dr. Sasha Romanosky *is a policy researcher at the RAND Corporation. Sasha was a Microsoft research fellow in the Information Law Institute at New York University, holds a CISSP certification, and is co-author of the Common Vulnerability Scoring System (CVSS). (sasha.romanosky@gmail.com).* ***Mr. Trey Herr*** *is a Senior Research Associate with the Cyber Security Policy and Research Institute. He is also a PhD candidate in Political Science at George Washington University. (rch760@gwu.edu).*

of these markets in order to reduce losses, and bring about more efficient investment in information security?

The Market for Threats

What drives cybercrime? The majority of computer-enabled or -supported crime is financially motivated, and thus the result of a rational cost-benefit analysis on the part of attackers.[8] The relative security posture across firms and the cost of acquiring and implementing malicious software (i.e., malware) can influence target selection by these criminals. Successful cyber attacks can therefore be considered a result of mismatched investment in information security. Attackers constitute a market for "threat," counterbalanced with a victim's market for security. In these markets, there exist two principal goods: malicious software and stolen data.

Goods: Malicious software used by criminals to gain access to a victim's information systems is composed of three parts, each of which can be developed, bought, and sold independently of each other[9]: a propagation method, exploits, and a payload.

The propagation method is the means of transporting malicious code from the origin to its target. This could be as simple as a mass email for spear phishing attacks or as complex as carefully crafted "dropper" software (code intended to infect a target machine and then retrieve additional malware from a command and control server elsewhere on the Internet). Exploits work in support of the payload and propagation method, taking advantage of software flaws that allow attackers to manipulate a software application or an entire computing system. The payload is code written to achieve some malicious goal on the target computer, such as deleting data, pilfering corporate intellectual property, or manipulating an industrial control system (ICS).

These different components are exchanged using various transaction types, in some cases rented, while in other cases sold outright.[10] One of the most popular means to distribute malware is via phishing, emails propagated by large collections of zombie computers called botnets. These botnets are usually rented rather than sold, and the machines in each "herd" of computers are maintained by an individual or small group that continually infects new machines in order to offset lost computers or expand their herd.[11] Stolen data comes in an even greater variety of forms; for example, credit card numbers are stolen, bundled, and sold through an ever-evolving mix of illegal underground marketplaces, some available only via the TOR onion routing protocol.[12] In addition, thieves may use the loot themselves, while in other cases the stolen data is sold to security researchers, or to corporations such as banks looking to detect fraudulent accounts.[13]

These markets for malware and stolen data are supported by several types of actors, described below.

Actors

Criminal organizations vary in size, purpose, and sophistication. Some are focused exclusively on espionage and have developed the means to distribute work internally, with different teams assigned to research and identify future potential targets, passing off their work to others for the development of malicious code, and yet more teams to package and deploy it.[14] Other groups, organized along the existing social networks of offline criminal organizations, pursue a wide range of criminal activities, using information obtained to conduct traditional identity theft, extortion, and financial fraud.[15]

Some groups retain a single function. For example, the process of "carding" (using stolen credit card information to reproduce cards and withdraw funds before the cards or their accounts are frozen) has emerged as a specialty activity in some circles. Small numbers of more knowledgeable "carders" tasked with stealing or otherwise securing credit card information then distribute these to large numbers of money mules (otherwise unknowledgeable low level individuals spread across regions and countries), who then withdraw funds from ATMs.[16] The goal for carder groups is to use purchased credentials to extract as much cash out of these accounts as possible, as quickly as possible, before banks begin to disrupt the process. Several of the largest groups devoted to stealing funds from stolen bank accounts with replicated credit card information are vertically integrated, responsible for every step of the

fraud process from theft to withdrawal.[17]

The market for threats assumes largely financially motivated actors, and does not consider strategically motivated actors who pursue political or military goals without regard for financial benefit. These activities, which may involve attempting to achieve destructive digital or kinetic effects, fall more closely under the military cyber operations topic rather than cyber crime. For financially motivated actors, however, there are established market mechanisms—a means to determine available buyers and sellers, to price the goods themselves, and establish the reputation and some means of transaction between actors. We discuss these dynamics next.

Market Dynamics: Much like the market for a used car or a new toaster oven, the market for cyber threat shares several underlying characteristics: trust, reputation, price, and competition. Unlike cars and toasters, however, buying and selling malicious software and stolen data takes place under a necessary veil of secrecy.

As there are few external means to compel buyers to provide payment, or sellers to provide their wares in the event of a fraudulent transaction, reputation plays a pivotal role. Some markets adopt a reviewer process much like Amazon, where other customers can comment on their experience with different malware components. In writing about purchasing freejoiner, a malicious payload that can steal personal data, for example, one such customer commented, "Purchased a freejoiner 2 and left very happy," while another wrote "Thank you for a FreeJoiner, is the best program in its class I have ever seen."[18] Some underground websites may compliment these user reviews with site moderators who verify products and transactions to track high quality sellers and remove scammers. Customer satisfaction matters; sellers of credit card information may offer bonuses if users buy certain quantities, or offer freebies to make up for already deactivated accounts.[19]

Another dynamic to consider is the price of goods within this marketplace. The cost of email account credentials, for example, has fluctuated in the past decade, ranging between $4 and $30 in 2007 and dropping to $0.50 to $10 in 2015.[20] This drop in prices may indicate oversupply, a surplus of available accounts, or less demand for email as a means of developing and sustaining attacks. Prices for custom features and revisions are added on top of the initial purchase by sellers who expect repeat business or who are selling a tool to users as part of a service. The "Pinch" malicious payload offers users a means to steal data from targeted systems in a variety of configurations. Though at one point Pinch's source code was posted online, the tool continued to be updated and sold on a regular basis for up to $30 per user.[21]

Competition plays a role in the market for threats as well. Where buyers can select between different sellers, the traditional competitive mechanics that decrease price and increase quality come into play, especially for malicious software components. One example is the evolution of SpyEye, a rival to the popular ZeuS malware which has primarily been used to target banking systems for user credentials but now includes a host of other features.[22] Early versions of ZeuS were relatively simple, but the emergence of SpyEye at a lower price point in the same forums to target the same customers resulted in a feature arms-race between the two payloads, with developers rushed to add more features to each in an effort to attract and maintain customers.[23] In 2010, just over a year after SpyEye's emergence, the two actually merged, with ZeuS folding into its rival's brand.[24]

Influencing the Market

There are often two opportunities for policy interventions—*ex ante*, or before the event, and *ex post*, after the event. *Ex ante* opportunities to shape the market for threat rest primarily on altering the market dynamics explained above. While targeting price seems an obvious first step, there are multiple byproducts to consider. Attempting to increase the price of malicious software components may make it less attractive for low-skilled attackers to acquire capabilities and could reduce overall demand, but such an increase may also incentivize new sellers to join the market, thereby increasing the variety or sophistication of what is available. For stolen information, there are similarly multiple effects from any action; attempting to increase the price of stolen information may reduce the

number of individuals willing to make purchases, but could increase the perceived value of such information, incentivizing more elaborate attempts to steal new credentials and card data.

An alternative approach may be to attack the reputation mechanisms, disrupting the tenuous chains of trust that link buyers and sellers for malicious software and stolen information. For example, law enforcement agents sometimes pose as sellers and falsify reviews, but can also set up alternative markets in an effort to drive users onto a smaller and smaller number of controlled platforms.[25]

Sowing distrust by seeding outdated/useless credit card or personally identifying information could also help disrupt these criminal markets as buyers are faced with an increasingly uncertain environment in which to spend limited resources. Operating in a market is difficult, especially where it takes place in a more clandestine context with few mechanisms to enforce transactions or guarantee contracts. The traditional information asymmetry between the seller who holds a good and the buyer who seeks to obtain it is made that much more burdensome as the market for cyber threats is fundamentally a den of thieves. With mechanisms to establish the reputation of, and trust in, buyers as willing agents and sellers as purveying the goods they advertise already fragile, law enforcement activities to disrupt these processes may yield outsize effects.

Ex post options are more common but somewhat more restrictive, focusing on punitive criminal measures for buyers and sellers as well as intermediaries like forum operators who provide a marketplace for these interactions. A conventional alternative to directly attacking the market for threats is to apply penalties to transpiring activities and prosecute buyers and sellers.

The primary legal vehicle for U.S. cyber criminal law enforcement is the *Computer Fraud and Abuse Act*, originally enacted in 1986 and amended several times since. The CFAA criminalizes conduct in two general categories: access to computer systems and activities on them. The nine main violations include "exceeding authorized access" to a computer system,[26] trespassing on a government computer,[27] and causing damage by intentional access either recklessly or with negligence.[28] There are limitations to the law, however. This includes a running debate within the courts over the definition of "authorized" access where there are at least three competing definitions: a) behavior taken to bypass existing and clearly evident security measures, b) any activity, including that by otherwise authorized users, which exceeds the authorized scope of operations on that computer system, and c) actions taken to obtain access to information in excess of that for which use of the computer system was originally granted.[29]

The Market for Security

There are many forms of government intervention that can be adopted in order to induce companies (and individuals) to invest in an appropriate level of information security, and optimize (but not necessarily eliminate) any harms caused by the kinds of criminal activities previously described.

Ex Ante vs. Ex Post: As mentioned, two familiar interventions are *ex ante* safety regulation (mandated standards), and *ex post* liability.[30] *Ex ante* regulation is considered a heavy-handed prevention mechanism that enforces a minimum standard of care in order to prevent or reduce harm (e.g., fire codes that define wall thickness and materials used in clothing or homes). These standards are useful when the harms are thought to be extreme (i.e., either catastrophic or miniscule) but widely distributed, affecting large numbers of individuals. Obviously, catastrophic harms (e.g., nuclear disasters) are worth preventing through regulation, but as are minor harms that are spread across thousands or millions of individuals. The reason is that the harm to any one individual may be small, but in the aggregate, it may be worth the burden of increased prevention.

Regulation can also be useful when the source of the harm is unknown. For example, in the case of health risks (e.g., pollution) or data breaches, often the offending company may not be known, and so it becomes worthwhile to mandate specific controls to prevent avoidable harms. However, its effectiveness is hampered when the regulated

inputs are only loosely correlated with the harmful outputs. For example, mandating two factor authentication and encryption on Health IT systems may be ineffective if health professionals share login information and remain logged in to applications, resulting in medical identity theft.

Nevertheless, monitoring compliance to a regulation may well be easier for an enforcement agency than estimating the amount of harm caused by a particular event. For example, it may be much easier to verify that a company has implemented basic security controls and passed a security audit than it is to measure the total loss from identity theft. This leads into a separate question of what manner of policy reforms are feasible rather than most effective.

Ex post liability, on the other hand, is meant to allow injured parties to recover any losses through civil litigation. The cost of defending against a lawsuit and the threat of future suits are expected to force companies to internalize any losses, inducing them to increase security prevention measures. Liability, however, becomes ineffective if the harms are either incalculable, unverifiable, or when the injuring party is unknown. Identity theft and privacy harms, for example, often suffer from these limitations; while courts have granted standing for plaintiffs in some cases of credit monitoring, these claims are more frequently dismissed where they argue increased potential risk of identity theft or fear of future harms.[31] However, a liability regime has the advantage of allowing firms to manage their information assurance (generally, any prevention measures) on their own, in ways that are most efficient for them. When they do properly bear the cost of their actions, they will naturally seek ways to reduce their total cost of any harmful behavior.[32]

Data Breach Disclosure Laws: As a result of losses stemming from data breaches, most states in the U.S. (as well as other countries) have enacted laws that require organizations to notify individuals when personally identifiable information has been lost or stolen. A primary goal of the laws is to empower consumers to take action in order to mitigate losses. A secondary goal is to force firms to internalize more of the cost of a data breach, thereby inducing them to increase their investment in security measures.[33]

The impact of these laws has yet to be fully examined, but existing research provides mixed conclusions; one study demonstrated an improvement in firm practices,[34] while another found only marginal reduction in the rate of consumer identity theft.[35] Critics argue that such laws inflict unnecessary costs for both firms and consumers if indeed firms already bear most of the loss,[36] or when lost data is recovered before it is even accessed.[37] Moreover, when the risk of harm is low, unnecessary notification may desensitize individuals, preventing them from acting when a serious threat does exist.[38] Further, consumers may be unable to properly respond to breach notifications, as the notices may present a substantial cognitive and psychological barrier to taking action, also causing them to under-react.[39] Alternatively, news media and the burgeoning market of identity theft prevention services may breed panic and confusion, causing consumers to over-react by unnecessarily purchasing such products, increasing their expected costs.

Cyber Insurance: Since the first data breach disclosure law was passed in 2003, thousands of breaches have been publicly disclosed, increasing costs to firms—costs against which they are preferring to insure. What has followed is a powerful and unforeseen consequence of fueling a market for cyber insurance.[40]

The defining characteristics of cyber insurance are: interdependent security, correlated failure, and information asymmetry. Some of these properties are common to all insurance markets, while others—and their combined effects—are unique to the risks of networked computing systems and cyber insurance. First, interdependent security reflects the degree to which the security of one computer network is affected by the compromise of another system (the breached system is said to impose a negative externality on the victim). For example, the security of Reagan National airport in Washington, DC may be compromised if luggage from SFO is not properly screened.[41] Correlated failures are where a single malicious event can cause failures across a host of systems; the loss of power at security monitoring company like ADT could

compromise the security of residences in surrounding neighborhoods. Finally, information asymmetry in the context of insurance reflects the familiar moral hazard and adverse selection problems; companies behave in a more risky manner when fully protected from loss and insurance carriers have difficulty differentiating between high and low risk clients.

Cyber insurance policies generally cover three categories of loss: first party losses, regulatory fines and fees, and third party liability. First party coverage includes losses stemming from outages or business interruption costs incurred due to a data breach, privacy violation, or security incident. Examples include breach notification costs, credit monitoring, public relations, forensic investigations, call center support, business interruption, and in some cases even extortion. Regulatory fines and fees cover sanctions brought by state or federal agencies (e.g., by the FTC or SEC). Third party liability coverage includes settlements, judgments, and defense costs due to civil litigation. Naturally, these policies also include many exclusions, such as discrimination, criminal or deliberate acts, patent infringement or violations of trade secrets, or acts of war, invasion or insurrection.

The data collected by insurance carriers affords them a unique advantage over any other entity—even government agencies—when it comes to assessing the benefits of different information assurance controls and practices. Recall that the critical questions are: which security controls are most effective at reducing risk? Is it better to have a firewall or an intrusion detection system? Is two-factor authentication really better than single-factor? If so, by how much, and how much of a discount in premium should a policy holder enjoy? To date, no single firm or government agency has been able to answer these basic, yet fundamental, questions.

Yet insurance companies are perfectly positioned because they possess the necessary data. Using their security assessment forms, policy and claims data, they can correlate the information assurance controls of an insured entity with loss outcomes. With sufficient data, the carrier could rank order security controls by effectiveness. This would, in effect, determine which information assurance measures are most effective at reducing loss. These answers could be invaluable at driving information assurance research, the market for cyber insurance, and ultimately the security posture of U.S. critical infrastructure.

Alternative Policy Devices: Taxes, subsidies, and nudging are additional methods of inducing efficient behavior. Taxes and subsidies are often thought to produce equivalent outcomes whether a policy maker taxes bad behavior or subsidizes good behavior (and in this way, each are considered efficient policies). However, taxes (or any form of sanction) will be less efficient as the cost of applying those sanctions increases. For example, a subsidy can simply be paid to those who comply, while noncompliance must be detected and enforced, which can be costly. Sanctions may be preferred to subsidies if the *threat* of sanctioning is credible, because the desired behavior is achieved at no cost.[42] Some have even suggested a "reversible reward" in which a subsidy is offered for compliance, but then in the event of non-compliance that same reward is used to penalize (perhaps through litigation or other sanction), thereby doubling the incentive mechanism.[43]

Nudging has become a very popular form of public policy.[44] It is a form of choice architecture that specifically exploits (rather than ignores) human cognitive biases in order to achieve outcomes that are thought to be in the best interests of the individual. For example, if students are more likely to fill up on foods that are presented first in a cafeteria lineup, then simply presenting healthier foods before fattening ones should create healthier plates without eliminating personal choice. Indeed, there is no reason nudging cannot be applied to the private sector for the purpose of appropriate information assurance investment; after all, companies (and government agencies) are run by people.

Information Security as Investment

Information assurance as the means to prevent compromise is fundamentally a question of security investment as firms seek to reduce the likelihood of an attacker stealing sensitive data or disrupting operations. On one hand, under-investment is less costly, it yields a greater number of successful attacks and is suboptimal

as firms lose valuable information and customers over the inability to protect their data and systems. On the other hand, over-investment can be similarly damaging as companies expend scarce resources with little to no return on improved security. An effort to thwart every single attack is likely impossible as there are no perfectly secure systems, especially given the necessary involvement of human operators. Framing information security as an investment, therefore, proposes that the purpose of government intervention is to support a market that encourages companies to find the optimal point between the cost of attacks and benefit of defensive information assurance measures.

Many consumer rights organizations and privacy advocates argue that companies are not spending enough on information assurance. In their eyes, this may be justified by the increasing rates and scale of software vulnerabilities and data breaches. This argument, however, rests on two conditions. First, it assumes that consumers cannot—or should not—take measures to protect their own data and computing devices. Like pedestrians looking to cross a busy roadway, do consumers, themselves, not also bear some responsibility for taking appropriate precautions when browsing the Internet, and protecting their personal data? Certainly, there are many circumstances when individuals are harmed through no fault of their own (e.g., theft of one's personal information from a data breach). However, there are also many situations where individuals *are* or *could be* empowered to take measures to protect their data (such as practicing proper browsing habits, the appropriate disclosure of personal information, password hygiene, laptop and data record storage, etc). And so, discussions regarding policies or regulations to force firms to increase cyber security should also be balanced with discussions of inducing *consumers* to take appropriate security and privacy precautions.

The second concern is that the argument that companies do not invest enough implicitly assumes that a world where companies *did* properly invest would experience *zero* data breaches or security incidents. Effectively, "appropriate" security, by that argument, implies "absolute" security. But as we have heard many times, perfect security is only achievable with zero utility (i.e., a broken computer is perfectly secure but entirely useless). Therefore, if we recognize that perfect security is neither practical nor efficient, and we instead seek to have both companies and individuals bear some responsibility for their actions, and invest in an efficient level of precaution (i.e. one that balances the incremental costs with incremental benefits), then this would describe a world in which both data breaches and security incidents existed.

The point is simply that the existence of security incidents could, in fact, reflect a state of efficient security investment. Just because we see some volume of data breaches or security incidents does not *necessarily* imply that companies (or individuals) are not *already* spending an efficient amount on data security. While increased spending may reduce security incidents, that additional cost of investment may be larger than the benefit from that investment. If efficiency is the primary goal, then before we answer the question of "*how* should we encourage companies to invest more?" we must first ask, "*should* we encourage companies to invest more?"

While some policymakers may applaud firms for managing information assurance just as with any other kind of risk they face (product, employee, corporate, etc.), there is an important consequence to this action. Namely, that by doing this, firms will (can and should) act in their own best interest. While this behavior is appropriate, these actions may ignore any harms they cause to consumers. That is, when firms cause harms to others but don't bear the burden of those costs, they act in a manner that is not in society's best interest.

In sum, the goal of a policymaker should be to optimize—not minimize—security incidents. That is, he or she should seek to balance the cost of a security measure with its benefit. Thus, the existence of data breaches and security incidents does not *necessarily* imply that companies are not investing in an efficient level of security. In fact, an absence of successful attacks leading to breach would likely imply excessive spending. People, like companies, are self-interested; we make decisions to maximize our returns and so should not expect companies to do otherwise (or begrudge them when they do). The challenge of stymieing cyber crime is finding the point where reasonable security investment yields appreciable

returns, and effective information assurance techniques can act to deter most attackers and prevent catastrophic incidents.

A Balancing Act

Structuring a policy response to cyber crime that encourages efficient investment in security and disrupts the market for threats is a difficult proposition, but progress is possible with an approach that recognizes the scarce resources available to both attackers and defenders. An important consideration for policy reform is the role of independent researchers and academics, who play an important function in identifying vulnerabilities and testing information security systems. These activities, like penetration testing and vulnerability disclosure, can sometimes appear uncomfortably similar to criminal activity at a high level, so a degree of nuance is required for any legal reforms that may impact their activities.

This paper serves as the third in a five part series developed to explain cybersecurity and the four large topic clusters it covers.

Endnotes

1) However, in some cases of cyber stalking and online harassment, outcomes can be tragic. See http://nobullying.com/six-unforgettable-cyber-bullying-cases/.
2) Goodin, D. (2008). IT Contractor Caught Stealing Shell Oil Employee Info. The RegisterUK.
Available at http://www.theregister.co.uk/2008/10/07/shell_oil_database_breach/.
3) McMillan, R. (2008). United Healthcare Data Breach Leads to ID Theft. Network World.
4) Hogan, M. (2008). Arrests Made in ID Theft Case, Sealy News. Available at
http://www.sealynews.com/articles/2008/09/23/news/news04.prt.
5) Federal Trade Commission. (2007). 2006 Identity Theft Survey Report.; Baum. K. (2004). Identity Theft, 2004. Bureau of Justice Statistics.
6) For example, Target has incurred $252 million in costs due to its data breach.See http://www.privacyandsecuritymatters.com/2015/02/target-data-breach-price-tag-252-million-and-counting/.
7) http://www.cl.cam.ac.uk/~rja14/Papers/toulouse-summary.pdf
8) Becker, Gary, (1968), Crime and punishment: an economic approach, Journal of Political Economy, Vol. 76 No. March/April, pp.169-93.
9) Trey Herr, "PrEP: A Framework for Malware & Cyber Weapons," The Journal of Information Warfare 13, no. 1 (February 2014): 87–106.
10) http://securitywatch.pcmag.com/none/309324-rent-buy-or-lease-exploit-toolkits-a-la-carte
11) http://www.symantec.com/connect/blogs/renting-zombie-farm-botnets-and-hacker-economy
12) http://krebsonsecurity.com/tag/tor-carding-forum/
13) http://krebsonsecurity.com/2015/04/taking-down-fraud-sites-is-whac-a-mole/
14) https://www.fireeye.com/resources/pdfs/fireeye-malware-supply-chain.pdf
15) http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf
16) http://krebsonsecurity.com/2014/06/peek-inside-a-professional-carding-shop/
17) https://www.eecs.berkeley.edu/~sa499/papers/fc2015.pdf
18) https://www.defcon.org/images/defcon-15/dc15-presentations/dc-15-holt.pdf
19) http://www.dynamicssouthwest.com/computer-crime-is-slicker-than-you-think/
20) http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services
21) https://www.defcon.org/images/defcon-15/dc15-presentations/dc-15-holt.pdf
22) http://krebsonsecurity.com/2010/04/spyeye-vs-zeus-rivalry/
23) http://www.csoonline.com/article/2463175/data-protection/the-making-of-a-cybercrime-market.html
24) http://krebsonsecurity.com/2011/02/revisiting-the-spyeyezeus-merger/

25) http://www.cnet.com/news/q-a-fbi-agent-looks-back-on-time-posing-as-a-cybercriminal/
26) 18 U.S.C. §§ 1030(a)(1), (a)(2), & (a)(4)
27) 18 U.S.C. §§ 1030(a)(3)
28) 18 U.S.C. §§ 1030(a)(5)(B) & (a)(5)(C)
29) http://www.americanbar.org/content/dam/aba/publications/Jurimetrics/summer2013/anderson.authcheckdam.pdf
30) See generally, Landes William, Posner, Richard, The Economic Structure of Tort Law, Harvard University Press, 1987; Shavell, Steven, Economics and Liability for Accidents. New Palgrave Dictionary of Economics, 2nd Edition, 2008; Kolstad, Charles, Ulen, Thomas, Johnson, Gary, 1990. Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements?, American Economic Review, 80(4), 888-901.
31) Romanosky, S., Hoffman, D. and Acquisti, A. (2014), Empirical Analysis of Data Breach Litigation. Journal of Empirical Legal Studies, 11: 74–104. doi: 10.1111/jels.12035.
32) See Romanosky et al. (2009) for a full discussion of how these interventions have been applied to breaches of personal consumer information.
33) Majoras, D., Prepared Statement Of The Federal Trade Commission Before The Committee On Commerce, Science, And Transportation {U.S.} Senate On Data Breaches And Identity Theft, June 16, 2005.
34) Samuelson Law, Technology, & Public Policy Clinic. (2007). Security Breach Notification Laws:
Views from Chief Security Officers. University of California-Berkeley School of Law.
35) Romanosky, S., Telang, R. & Acquisti, A. 2011. Do Data Breach Disclosure Laws Reduce Identity Theft? Journal of Policy Analysis and Management, 30(2), 256-286.
36) Lenard, T. and Rubin, P. (2005). Slow Down on Data Security Legislation. Progress Snapshot
1.9. The Progress & Freedom Foundation.
37) Id at 30.
38) Id.
39) Romanosky, S. & Acquisti, A. (2009). Privacy Costs and Personal Data Protection: Economic and Legal Perspectives of Ex Ante Regulation, Ex Post Liability and Information Disclosure. Berkeley Technology Law Journal, 24(3)
40) A version of this article appears in Romanosky, S, (2013), Comments to the Department of Commerce on Incentives to Adopt Improved Cybersecurity Practices
Docket Number 130206115-3115-01. Available at http://www.ntia.doc.gov/files/ntia/romanosky_comments.pdf
41) Geoffrey Heal, Howard Kunreuther, Environmental Assets & Liabilities: Dealing with Catastrophic Risks (2009).
42) Donald A. Wittman, Liability for Harm or Restitution of Benefit?, 13 J. Legal Stud. 57 (1984)
43) Reversible Rewards, 15 American Law and Economics Review 156 (2013) (with Anu Bradford)
44) http://www.tandfonline.com/doi/abs/10.1080/13571510903227064

Defense Technology Program Brief

About The Defense Technology Program

A revolution is taking place in the nature of warfare. The proliferation of ballistic missiles and weapons of mass destruction has given rogue states and terrorist groups unprecedented access to potentially devastating capabilities, while space and cyberspace have emerged as distinct new arenas of strategic competition. The American Foreign Policy Council's (AFPC) work in these areas is aimed at helping U.S. offcials understand and respond to this new, and increasingly complex, threat environment.

For more information about the program, please contact Richard Harrison, Director of Operations and Defense Technology Programs at Harrison@afpc.org.

About AFPC

For over three decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

AFPC Mission Statement

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:

- providing primary source information, as well as policy options, to persons and organizations who make or influence the national security and foreign policies of the United States;
- arranging meetings and facilitating dialogue between American Statesmen and their counterparts in other countries; and
- fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.

CONTACT

509 C Street NE
Washington, D.C. 20002
Telephone: 202.543.1006
Fax: 202.543.1007
www.afpc.org