OPEN TECHNOLOGY INSTITUTE
NEW AMERICA

Case Study | 2016 | RELEASE 1.0

Cascades:

The Anonymous Hack of HBGary (Teaching Note)

This teaching note was created as part of the Open Technology Institute's (OTI) effort to create a curriculum focused on how digital technology is transforming public policy and governance. It is intended for use in a classroom setting.

CASCADES

"Cascades: The Anonymous Hack of HBGary," a New America case study, captures how Anonymous, a prominent collection of hacktivists, penetrated HBGary Federal, an IT security company that sold its services to the U.S. federal government. The case begins in January 2011, one month before the hack, when HBGary Federal CEO Aaron Barr unveiled a plan to identify the names of Anonymous's leaders. The case then provides several pages of background on HBGary, IT security, hacktivism, and public policy in this realm before delving into Barr's effort to implement his plan and the implications of his actions. Specifically, the remainder of Part A details HBGary Federal's financial woes, how Barr pursued his research of Anonymous despite protests from his staff, and how he publicized his efforts to *The Financial Times*.

Part B then narrates how Anonymous responded to Barr's research by exploiting several weaknesses in the company's IT security defenses to deface the firm's website, gain access to tens of thousands of the company's e-mails and internal documents, and release (among other things) Barr's social security number.

Finally, Part C describes the aftermath of the attack—including Barr's resignation and the sale of HBGary, Inc.—and draws on expert interviews to identify some of the broader issues the attack raised and reflects.

In capturing Barr's research and the response it prompted, the case aims to animate student discussion around three main questions. First, why is the Internet difficult to secure? Second, how can technological and human/cultural flaws "cascade" to create true crises, as was the case with HBGary? Third, what can society as a whole and policymakers specifically do to mitigate some of these risks?

The teaching note that follows explains these questions in more detail and identifies the data in the case that is designed to inform classroom discussion surrounding each of these issues. It also contains recommended readings that faculty might consider pairing with the case.

Question One: Why is the Internet difficult to secure?

At one level, the case is setup to illuminate why the Internet is difficult to secure and why IT security is such a major issue. Specifically, it contains data on five issues that faculty may choose to highlight in class discussion.

The first is the significance—or massive scope—of the Internet, not to mention the rapidity with which it has attained such social, financial, and political importance. As the background section of the case notes, a report published in 2011 found that the Internet had been responsible for more than 20% of GDP growth in mature economies over the previous five years. At the same time, social media use—particularly Facebook membership—skyrocketed.[1] Threats on the Internet are potent in no small part because the Internet has become integral to society.

A second factor is that there are many forces and actors that use the Internet and are capable of inflicting damage. The case alludes to a number of them (including cybercrime), but it focuses primarily on hacktivism. As the background section of the case notes, experts have yet to agree on a precise definition of this phenomenon. As the case also establishes, the difficulty of parsing the meaning of hactivism complicates efforts to depict whether or to what extent it is nefarious. Nonetheless, the efforts of hacktivist organizations—including Anonymous, the group upon which the case focuses most closely—can represent a legitimate threat to the ability of targeted companies and organizations to operate their websites and (in some cases) secure their data.

A third issue is the range of techniques that hacktivists and other groups can employ to affect or damage an individual or organization. Drawing on the expertise of Harvard Professor Jim Waldo, Part B of the case highlights several of these methods. One is an SQL injection.[2] Another is employing rainbow tables and other tools and techniques to decrypt passwords. Finally, Distributed Denial of Service Attacks can allow hacktivists to disrupt an organization's website. By highlighting just a few of these techniques, the case provides a window onto the wide range of tools hacktivists and other groups can employ.

A fourth factor is that the IT security sector—the very industry designed to secure the Internet—has several core weaknesses. As the background section of the case explains, these include the fact that some IT security companies overhype their abilities and that many firms are targeted during attacks. The case also illustrates another issue: many IT security companies, despite being in the business of technology security, often have poor IT security themselves.

Finally, experts disagree about why the Internet is unsafe and what therefore needs to be done to make it safer. As the background section of the case notes, some argue that the key problem is technological and, in particular, that the Internet developed so quickly that developers did not have a chance to create strong safeguards. Others emphasize that it is primarily up to users themselves to make good decisions about what they download and (more broadly) how they use the Internet. In short, there is a foundational disagreement about whether and to what extent Internet security issues stem from human flaws, technological shortcomings, or some combination of the two; and without a sharp understanding of why the Internet is dangerous, it is difficult to pinpoint how to make it safer.

For additional reading, see:

Coleman, Gabriella, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, Verso: London, 2014.

Olson, Parmy. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*, Little Brown and Company: New York, 2012.

Question Two: The Danger of Cascades

The case is designed to educate students about not just the different phenomena that can make the Internet unsafe but also the dangers that can arise when those factors interact and "cascade" to create catastrophic consequences. In particular, the case illustrates two cascades that occurred at HBGary, Federal: the first involved a combination of technological loopholes; the second blended human error and characteristics of the organization's culture.

One of the goals of Part B of the case is to illuminate that HBGary not only had a number of loopholes in its IT security but that these gaps acted as a series of "dominos" that created a dangerous chain reaction. Specifically, the SQL injection (the first domino) allowed the hacktivists to access the password table. The second domino—the company's use of a fairly simple hashing function to encrypt its password(s)—allowed the hacktivists to crack the passwords of several employees, including CEO Aaron Barr. Finally, that some employees—including Barr—used the same passwords for multiple accounts allowed the hacktivists to gain far deeper access to HBGary's data/documents, as well as the personal accounts (e.g., Twitter, LinkedIn, etc.) of Barr. The broader takeaway is that security flaws do not operate in isolation; in point of fact, because they are connected, they can quickly escalate from a small hole to a gaping break in a company's IT security defenses.

A similar cascade can occur with human and organizational behavior. Beginning with the introduction to Part A, which captures how Barr and HBGary Federal were under enormous financial pressure, the case prompts students to consider how external pressure can lead to questionable behavior. Specifically, to stabilize the ailing firm, Barr decides to investigate one of the most prominent collections of hacktivists in the world; presses ahead when a staff-member warns him that his analysis is flawed; and then publicizes his efforts, a strategy which both signaled his plans to the hacktivists and, one might argue, was likely to prompt a reprisal. The implication is that organizations need to consider not just how their IT defenses interact with one another but also how their organizational culture and the personalities that shape it affect the company's vulnerability.

For additional reading, see:

Bright, Peter, "Anonymous Speaks: The Inside Story of the HBGary Hack," *ArsTechnica*, February 15, 2011, available at http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/ (accessed on September 30, 2015).

Question Three: Public Policy Implications

Finally, the case prompts students to consider the public policy implications of the challenges surrounding IT security. More importantly, it encourages them to consider what, if anything, governments can do to make the Internet safer. It accomplishes this in part by illuminating the challenges of policing the Internet. As Part A discusses, this includes the fact that the Internet and many IT security threats span political borders and often bring U.S. officials in contact with countries and actors with which the United States has tense relations. Another challenge is that the domestic regulatory landscape is fractured, with an array of agencies—ranging from the Department of Homeland Security to the Central Intelligence Agency—having involvement in IT security. Yet another difficulty involves the private sector, which plays an integral role in IT security but with which the U.S. government is still exploring the best ways to collaborate.

Nonetheless, the case also points to some ways that the U.S. government can overcome these challenges. In particular, Part C describes how the Anonymous hack of HBGary eventually prompted a call for a Congressional inquiry; focusing specifically on some of HBGary's business plans, the possibility of a probe provides an example of another regulatory approach. The case also draws on expert voices—including technology security author and *Reuters* reporter Joseph Menn—to capture the importance of increased dialogue to identify possible paths forward. These include extreme approaches—such as the militarization of the Internet—as well as more incremental techniques that recognize the centrality of the Internet and its security to the next generation and experiment with ways to balance safety and freedom. Melissa Hathaway, formerly the acting senior director for cyberspace at the National Security Council and a cybsersecurity advisor to Presidents George W. Bush and Barack Obama, also highlights the importance of encouraging policymakers to consider both the economic and security implications of investments in technology infrastructure and IT more broadly.

Regardless of the approach policymakers employ, the case aims to leave students with a strong impression of the centrality of IT security to all organizations—public and private. It therefore concludes with a quotation from Menn identifying this phenomenon as one of the most important issues of the 21st century and an insight from Hathaway, who notes that even though leaders are inheriting 25 years of problems, they do not have 25 years to address them. The implication is that policymakers need to have a sense of urgency and must develop an efficient and impactful approach.

For additional reading, see:

"Cyberspace Policy Review: Assuring A Trusted and Resilient Information and Communications Infrastructure," The White House, May 8, 2009, available at https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed on September 24, 2015).

Hathaway, Melissa, and Stewart, John. "Cyber IV Future: Taking Control of Our Cyber Future," *Georgetown Journal of International Affairs*, July 25, 2014, available at http://journal.georgetown.edu/cyber-iv-feature-taking-control-of-our-cyber-future/ (accessed on October 28, 2015).

Menn, Joseph. *Fatal System Error: The Hunt For The New Crime Lords Who Are Bringing Down The Internet*, Public Affairs: New York, 2010.

Index

[1] James Manyika and Charles Roxburgh, “The Great Transformer: The Impact of The Internet On Economic Growth and Prosperity,” McKinsey Global Institute, October 2011, available at http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_great_transformer (accessed on September 23, 2015).

[2] For a more detailed explanation of SQL injections and other technical terms, see Part B of the case study.