ISN
ETH Zurich

13 February 2015

Sony, the Internet of Things, and the Evolving Cyber-Threat

Do recent cyber-attacks — including North Korea's against Sony and a Stuxnet-style attack against a German steel works — suggest that the nature of the cyber-threat is escalating? Chris Bronk thinks so. That's because advances in computing and the revenue-driven culture of corporate hierarchies are undermining the implementation of much-needed security measures.

By Christopher Bronk for ISN

Because of their great frequency and increasing significance, cyber security events continue to rise on the policy and national security agendas of national governments and international organizations. While computer security efforts were once primarily concerned with general threats and non-specific actions such as widely propagated computer viruses or email phishing campaigns designed to indiscriminately harvest access to many computers for relatively benign purposes (such as sending spam email), attacks have grown increasingly sophisticated and precisely targeted.

Efforts to compromise systems are now often tied to economic or political espionage efforts or even covert action designed to produce specific outcomes. Acknowledging these developments, it is important to consider the implications of two recent cyber- attacks: the breach at Sony Entertainment, and another that didn't make headlines to the same degree, the attack on an industrial plant at a German steel company in December. For organizations that represent viable targets for foreign governments, corporate rivals or activists groups, these attacks highlight the importance of balancing organization-wide incentives to bring in revenue with the growing imperative to improve security.

Sony's woes

In December 2013, the hack making news was Target's data breach . Crafty thieves emplaced software on cash register terminals and purloined millions of customer records. Shoppers swiped their magnetic cards and unknowingly gave away credit and debit card data for weeks.

In 2014, the big breach at Christmastime was Sony's. Materials compromised in the attack included everything from internal documents and email to digital copies of unreleased feature films . The hackers that went after Sony caused such fear that when they threatened physical violence against theaters showing *The Interview*, a satirical farce involving an assassination plot against North Korean leader Kim Jong Un, most balked at showing the film.

The U.S. government reaction to the Sony breach amounted to calling the matter a crime, launching an investigation, and issuing a vague threat against Kim's regime that some sort of response may be undertaken. U.S. officials openly blamed North Korea for the Sony breach, and even President Obama spoke publicly on the matter, castigating the North Koreans for the act and shaming large theater chains for caving in to the threat of violence.

As with most other major cyber attacks, alternate theories arose regarding the hack. Representatives of the ever-growing cyber intelligence and malicious software analysis industries said the allegations against Kim Jong-Un's regime were premature. The Sony hack was likely an inside job perpetrated by a disgruntled employee, they argued.

Eventually a strong counter-narrative would emerge from the Snowden archives, published by *der Spiegel* and additional claims published in *The New York Times* . The U.S. government's final, if not-for-attribution, word was that it knew of Pyongyang's complicity because North Korean systems had been compromised by U.S. cyber intelligence operatives.

New SCADA hacks

While Sony's woes made good hacker theater, another incident, at a steel plant in Germany, should cause greater concern. In December, representatives of the BSI, the country's cyber defense agency, reported that the control systems computers of a steel works were hacked in a manner that caused an emergency shutdown of a smelter, severely damaging it .

Attacks on Supervisory Control and Data Acquisition (SCADA) systems are especially worrisome because one of the key growth areas in the IT industry is in embedding networked computers into machinery, from production lines to home appliances. This new computing infrastructure, labeled the Internet of Things (IoT), promises new efficiencies and capabilities, but also increases the attack surface open to cyber attack – from laptops and smartphones to home thermostats and offshore oil rigs.

Worryingly, evidence continues to emerge that SCADA system hacks are occurring and that the IoT is riddled with security holes. Beyond the grandfather of these events, the Stuxnet attack against Iran's nuclear enrichment facilities, the German event adds to a growing list of possible or probable SCADA cyber attacks. (So does a recent research case study on hacking traffic lights.) This is a bigger concern than the gossip and anxieties of studio executives.

In the same vein, new evidence has come to light regarding a 2008 pipeline explosion in Turkey , which occurred only 3 days before Russia invaded its neighbor Georgia. For years we assumed this was an act of terrorism. Now there is an alternate thesis involving the manipulation of pumping infrastructure and the pipeline's surveillance system.

The new 'great game'

At least since Stuxnet, if not before, a geopolitical contest for control of cyberspace has been taking shape. The cyber vector in international conflict is now fully primed, and a variety of actors now employ cyber means to achieve their ends. Over time, they will do so with increasing sophistication. While most of the traditional levers of geopolitical competition remain available to states, 'cyber' is one that works.

Cyber attacks can now break physical things, and most organizations are woefully unprepared for that development. The security model of buying hardware to counter specific or individual threats is often inadequate against an increasingly well-educated, creative, and highly-motivated cohort of malicious

hackers. Equipped with dynamic and ever-advancing tools, highly skilled cyber defense professionals must face these operators, much as intelligence analysts of great skill and talent toil to stop terrorists with far less in the way of training or preparation. Although education has come to the fore, teaching and learning take time and more capable practitioners are needed urgently.

Moving to the larger geopolitics, there are now many hacking cases in which a strong political motive may be present but definitive evidence linking the attacker to the attack is difficult to find. This was the case with the *Shamoon* attack against Aramco . Iran is assumed to be the culpable party, but a clear connection between its supreme leader and the hack that took down 35,000 computers in minutes has not come to light. Conversely, numerous Pentagon PowerPoint presentations leaked by Edward Snowden have provided far more definitive evidence about U.S. intelligence activities in cyberspace.

What can or should be done ?

Despite the security pitfalls abundantly visible today, computing marches forward. Big data is unlocking advances in health care. Process control optimizes critical infrastructure: pipelines, electricity distribution, and integrated logistics. Digital transactions are the backbone of global investment banking and the lifeblood of small business operators alike. All of these things can be hacked, and the consequences can be serious.

In major corporations, the awareness of senior leadership about the cyber threat is rising. What is not changing quickly enough are organization-wide incentives for actors, especially in upper management, to implement enhanced security measures. Indeed, in far too many cases, the imperative to improve security remains at odds with the imperative to bring in revenue. Too often, corporate culture emphasizes the latter at the expense of the former.

That is the core of the problem for Sony, for our anonymous German steel company, and for any other firm that represents a viable economic target for a foreign power, competitor firm, or hacktivist group with an agenda. Organizational cyber security is a fatalistic culture because, in some ways, it resembles the intelligence or counter-terrorism business. Successful defenses do happen, but they are rarely made public. It is only when something goes wrong, and the heads begin to roll, that the cyber-threat gets the attention it deserves.

For more information on issues and events that shape our world, please visit the ISN Blog or browse our resources.

Christopher Bronk is the Baker Institute fellow in technology, society and public policy (TSPP) at Rice University. He previously served as a career diplomat with the United States Department of State on assignments both overseas and in Washington, D.C. He holds a Ph.D. from The Maxwell School of Syracuse University and studied international relations at Oxford University.

Publisher

International Relations and Security Network (ISN)