SCHOLARS
STRATEGY NETWORK

Cybersecurity Incidents Can be Unwelcome Wakeup Calls for Unprepared Agencies

Jeremy Straub, North Dakota State University-Main Campus

Several large-scale cyber breaches have shown how vulnerable our government agencies are from a growing digital threat. WikiLeaks' 2013 release of government materials provided by Edward Snowden exposed classified NSA files to the public. That same year, the Office of Personnel Management breach placed key information about most of the United States' security clearance holders into the hands of potential adversaries. In both cases, the agencies contributed to the breach through poor cybersecurity. To avoid future catastrophic incidents, agencies should eliminate unneeded data collection and storage, exercise increased diligence with records, and build trust through public relations activities that explain their operational and security practices.

The Insecure Cybersecurity Environment

With data breaches happening every day and growing threats that hold data hostage for payment, the question is not if or even when another breach will happen. The question is what company or agency will be breached next, what data will be stolen, lost, or held for ransom, and how bad the fallout will be.

Understanding this growing escalation, former Secretary of Defense Leon Panetta warned that the long game of these attacks could lead to a Cyber Pearl Harbor. This basic concept refers to an unexpected attack that energizes the public with a need to respond. As with the actual attack on Pearl Harbor, the warning signs for any number of future Cyber Pearl Harbor attacks might already be present.

The Threat of Foreign State Actors to Agencies

The United States faces a wide variety of potential cyber attacks from foreign adversaries. These range from attacks that seek to capture secret information from government servers—like the Office of Personnel Management breach—or disable key computer functionality to attacks against infrastructure to online misinformation campaigns. Foreign actors have been deemed responsible for election interference, numerous instances of data theft, interfering with fuel transportation, and tampering with water supplies. Despite all of this, nothing has risen to the level of a Cyber Pearl Harbor, in terms of energizing the public to rise-up and demand that the government take action.

The next attack could be immensely destructive. It may start with an adversary just seeking information. But the opportunity to disable the system may present as just too good to pass up—or maybe the adversary does not even fully understand what system they are in, and they disable key services inadvertently. An adversary disabling air traffic control, for example, risks planes crashing in mid-air—and certainly brings the speed of air travel to a crawl. Disabling the power grid in winter risks causing deaths from freezing, while attacking a nuclear power station risks the discharge of radioactive materials or even a reactor meltdown.

The Ramifications of a Pearl Harbor Incident

On top of impacts to the public, a Cyber Pearl Harbor incident could be tremendously detrimental to an agency. The Snowden leak galvanized the public and the U.S. Congress against the government surveillance program and also caused changes in how and where records are stored by private firms. This phenomena, known as the "Snowden Effect," is a result of many overseas individuals, firms, and governments no longer wanting their data in the United States and subject to U.S. surveillance.

An agency that is subject to an unexpected and mass breach, at best, will find it difficult to regain the public's trust. Key to that trust rebuilding will be whether the agency was caught "in the act" of something nefarious, and whether the attack demonstrates poor practices. Of course, public perception will also be shaped by what is compromised and its impact on individual and national security.

Agencies that rely on public support to obtain resources and those that provide direct services, or rely on public cooperation for their work, would likely be the most impacted by a breach. Individual citizens might choose not to use agency services, not seek employment with the agency, and object to the agency holding their information. Significant public outcry could cause policy makers to restrict agency operations or funding in line with public demands.

Avoiding Pearl Harbor Cybersecurity Incidents

Agencies seeking to avoid Pearl Harbor cybersecurity incidents should, of course, focus on the security of their electronic assets and the digital, physical, and personnel security required to protect them. Other concrete steps to avoid catastrophe include:

- Agencies would be well advised to not engage in activities that could be seen as covert or nefarious, or that cannot be explained by their mission. Activities that access individuals' personal information should be publicly disclosed—at least conceptually, if possible—and have effective oversight to prevent misuse and scope creep.

- Agencies can also prepare themselves for the likely inevitable breaches to occur. First, they can reduce the amount of data stored to the minimum needed to perform their public function. This means only collecting the records and individual pieces of data specifically required for a particular transaction and reducing document retention policy periods to maintain data records for only as long as they're needed for a transaction, possibly removing some data immediately after transaction completion and disposing of the remaining data at a later time. Data that an agency does not have cannot be hacked.

- Agencies can train staff members to create and treat every agency record as if it could end up in the public's hands by avoiding grotesque notations, stereotyping and other offensive content. Writing and curating internal records like they will be read by the public doesn't just help with cyber breaches; it can also be helpful for records subpoenaed for lawsuits, those obtained through open records requests, and for other purposes.

- Agencies should actively engage and communicate with the public about their mission and the methods and tactics they use to achieve it. For a truly successful attack, an adversary will act on a goal, cause a Cyber Pearl Harbor Event, and produce a Cyber Pearl Harbor Impact. Technological mitigation can reduce the likelihood of the event; however, agency positioning and public messaging— both before and after the event—can determine whether the adversary is successful in creating their desired impact . Agencies, thus, have a significant opportunity to control the fallout from a breach with their pre and post incident response

Read more in Jeremy Straub, "Defining, Evaluating, Preparing for and Responding to a Cyber Pearl Harbor." *Technology in Society* 65 (May 2021).