Above My Pay Grade: Incident Response at the National Level

Jason Healey

Incident response for information security is a well-understood discipline which provides signficant resources to help newcomers to the field understand what to do after an intrusion or denial-of-service attack. Professional responders understand all about assessing the impact on an affected organization, finding traces of the attacker, stopping and mitigating the attack, and even helping determine who might be responsible.

About the Cyber Statecraft Initiative

The Atlantic Council's Cyber Statecraft Initiative focuses on demystifying the overlap between national security and cyber security to foster international cooperation and understanding of new forms of cooperation and conflict in cyberspace.

This effort was made possible by generous support by The Morganti Group Inc.

Unfortunately, for the very worst incidents, such as those are not isolated but an actual conflict, with national security implications, there is a very different process, one focused on Washington, DC. It is both poorly understood outside of the Beltway and there are few materials to inform outsiders about its intricacies.

This white paper, and the associated talk at Black Hat USA 2013, will give traditional incident responders a sense of the national security response and its strengths and weaknesses.

Imagine there has been a startlingly large campaign of cyber attacks disrupting the finance sector, affecting major banks as well as exchanges and the underlying infrastructure providers, such as clearing houses which ensure that shares and money change hands appropriately after each trade. The attack is worse than anything ever seen to date and has lasted for several hours already.

Jason Healey is the director of the Cyber Statecraft Initiative of the Atlantic Council and editor of the first cyber conflict history book, A Fierce Domain: Cyber Conflict from 1986 to 2012. He created the first Computer Emergency Response Team and coordinated the response to incidents affecting the finance sector, as vice chairman of the Financial Services Information Sharing and Analysis Center. He was a cyber policy director at the White House from 2003 to 2005.

The Finance Sector Response

The affected organizations would individually initiate their own crisis management procedures, including calling together their Computer Emergency Response Team. As the situation is serious, they would quickly escalate to include senior business leadership to help assess the impact to the business and assist in the response.

Once it was recognized as an attack, each firm might contact law enforcement, especially if it were seen as an intrusion or other obvious crime. Each organization would likely either contact the Federal Bureau of Investigations or the United States Secret Service, depending on the relationship between individuals in the security organizations of the banks and the local field office.

While the business side of each affected organization would contact their counterparties in other banks and the exchanges, the CERT team would report the incident to the Financial Services Information Sharing and Analysis Center (FS-ISAC).

The FS-ISAC is an operational organization, which usually would not handle financial or policy decisions. Accordingly, the action would soon pass to the Financial Services Sector Coordinating Committee for Critical Infrastructure Protection (FSSCC). The FSSCC is comprised of senior leaders from across the private-sector financial sector, including the exchanges, clearing and settling organizations, major banks, credit card companies, and the like.

The FSSCC would work to coordinate the response within the financial sector, working closely with government regulators and financial officials who sit in the Financial and Banking Information Infrastructure Committee (FBIIC), the Government Coordinating Committee of the NIPP. Chaired by Treasury, the FBIIC has senior representatives from the Federal Reserve Board or Governors, Securities and Exchange Commission, and other financial agencies.

Separately and together the FSSCC and FBIIC coordinate and make decisions to respond to the disruption. These groups would help advise on whether markets should stay open, guide or direct responses at individual firms, seek regulatory relief where needed, and assist the flow of information between firms and between the private and public sectors.

If the disruption were particularly severe, the President's Working Group on Financial Markets – comprised of the Secretary of the Treasury, the Chairman of the Federal Reserve and other of the highest-level officials – would convene and make decisions to guide the markets as they would for any kind of major disruption.

The Cyber and National Security Responses

In addition to helping the finance sector respond, the FS-ISAC would also inform other ISACs of the disruption and pass the alert to the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). NCCIC would quickly pass the information to the other cyber operations and watch centers including at Cyber Command and the National Security Agency.

At the NCCIC, with representation from all major Federal departments and agencies, the official government response would begin to counter the cyber attack causing with this operations center alerting and coordinating all departments and the major telecommunications providers. The NCCIC, including US-CERT would focus on technical sharing, understanding attack vectors, and how to mitigate the attack.

As the scale of the incident became clear, the NCCIC would escalate within the Department of Homeland Security, including the Cyber Unified Command Group up to the Secretary.

If higher level coordination was still needed, especially to handle difficult national security policy questions, DHS would escalate up to the National Security Council staff's Cyber Response Group, overseen by the White House's Cyber Directorate. From here, the cyber incident would be treated more and more like any other kind of national security crisis, with a dedicated "interagency" process, involving senior officials from all relevant agencies.

If the incident were indeed dire, or the government had to make the most serious policy decisions, the incident would be escalated further, up to the Deputies Committee (DC) and Principals Committees (PC) of the National Security Council including the President of the United States. The DC is the primary national-security decision body of the US government and meets dozens or hundreds of times a year to tackle the most difficult policy and operational questions. If the DC, comprised of the deputy secretaries of the national security relevant

agencies, cannot agree, they kick the problem up to the Principals Committee, with the President and secretaries.

This is exactly the kind of escalation path used if there is a coup in an important country or a terrorist attack on US forces overseas: rapid escalation up the NSC, supported by the White House Situation Room, to get the most senior decision makers involved in a well-known and long-tested process, supported by dozens if not hundreds of staff officers producing decision-support material. The president or National Security Advisor could be in the Situation Room chairing a Principals Committee within an hour of a major cyber incident. These senior-most US decision-makers can reach out to any place within the government or, indeed, call directly to foreign heads of state or government to seek cooperation or deliver demands.

Accordingly, many questions that seem vexing at the technical level actually are far more tractable, such as "what if we can't be absolutely sure about attribution?" or "how do we decide whether to shoot back?" The national security leadership at a DC and PC all of the time have to face make difficult decisions in the face of uncertain and spotty information.

One of the reasons this process can work so well is that the worst-impact cyber conflicts are generally caused by nations, not individuals, so understanding state-to-state security dynamics is of at least as much importance as cyber knowledge. Also, cyber conflicts tend not to be "network speed" but unfold over multiple attacks over weeks, months and even years. So even if the response process is not fast enough to stop individual attacks, it has a chance to stop unfolding campaigns.

Of course, this process does not ensure they will make the correct decision, but it helps ensure the most facts and options can reach those with the best experience in the shortest time. It can also get overwhelmed, such as if the United States faced a true 'cyber war' which caused hundreds of casualties or significantly degraded the US economy or infrastructure. Here the Department of Defense, not DHS, would be in charge and there has been little solid thinking on how they might coordinate the nation's private sector defenses. There would probably be no fewer than five four-star generals, all feeling they had a significant role in the nation's defense and a right to the President's ear, not even counting the many cabinet secretaries, state governors and CEOs.

Unfortunately, not all nations have such a robust system. China, for one, seems to lack a similarly complete process to link geeks and wonks for cyber incident response. Although interagency coordination is relative mature and improving – allowing the Ministry of Public Security (the overall lead) to communicate rapidly with the technical incident responders at CN-CERT and with the Ministry of Foreign Affairs and People's Liberation Army – China watchers are increasingly seeing a dangerous institutionalized disconnect between these mid-level officials and their political (and Party) leadership.

There is no clear link, as in the United States, for interagency experts to pass information up to the nation's leadership – or for those leaders to quickly get answers in fast-moving crises, such as in response to questions from Washington, London, or even Moscow. Conflicts and competition involving China in cyberspace thus will only become less transparent, more unstable, and more difficult for both sides to signal each other. The world will be safer once China, the world's burgeoning new power and clear cyberspace giant, is able to more effectively deal – both technically and politically – with cyber incidents.

The United States has in place a potentially very effective system to respond to large-scale security incidents. Fortunately, it has not been too stressed with fast-moving cyber conflicts. Of course, this is likely just a matter of time, though there is still time for technical incident responders to understand this national security system and its implications for them.