October 19th, 2021

TLP White

This week, *Hacking Healthcare* begins by examining the outcome of the recent international summit on ransomware hosted by the White House. Next, we assess the Australian government's new *Ransomware Action Plan* to see how it compares to other government efforts. Finally, we break down a recent joint United States government agency advisory on critical infrastructure cyberattacks and assess how it may influence administration and congressional actions in the healthcare space.

Welcome back to *Hacking Healthcare*.

1. **White House International Ransomware Summit**

   On October 13th and 14th, the White House convened ministers and representatives from 30 countries and the European Union to discuss the "escalating global security threat from ransomware."[1] The two-day meeting ended with a joint statement covering general efforts and commitments related to resilience, countering illicit finance, ransomware disruption and law enforcement actions, and international diplomacy.

   Below is a quick summary of the main points of each section:

   Resilience: According to the joint statement, building out resilience requires "effective policy frameworks, appropriate resources, clear governance structures, transparent and well-rehearsed incident response procedures, a trained and ready workforce, partnership with the private sector, and consistently enforced legal and regulatory regimes."[2] However, basic cyber hygiene and information sharing between ransomware victims and law enforcement were the two issues highlighted most strongly.

Countering Illicit Finance: This section stressed the importance of international cooperation to tackle the underlying infrastructure that allows ransomware to be profitable. This included a focus on enhancing "the capacity of our national authorities, to include regulators, financial intelligence units, and law enforcement to regulate, supervise, investigate, and take action against virtual asset exploitation."[3]

Disruption and Law Enforcement: The joint statement acknowledged the need for increased international cooperation among law enforcement, national security authorities, and cybersecurity agencies to tackle the transnational nature of ransomware. In particular, the section highlighted the importance of "[taking] appropriate steps to counter cybercriminal activity emanating from within our own territory and impress urgency on others to do the same."[4]

However, the most important point made is almost certainly the statement that the countries taking part in the summit "will consider all national tools available in taking action against those responsible for ransomware operations threatening critical infrastructure and public safety."

Diplomacy: The diplomacy section advocated for two specific actions. First, it underscored how coordinated capacity building is a meaningful way for countries to address ransomware. Second, it stressed "coordination of action in response to states whenever they do not address the activities of cybercriminals."[5]

Action & Analysis
Membership required

2. Australia Releases Ransomware Action Plan

Last week we covered how the governments of the Netherlands, United Kingdom, and United States were attempting to respond to the continuing threat posed by ransomware. This week, it is the Australian government that has released a significant policy document on the topic. While not a direct product of the aforementioned White Housel summit on ransomware, Australia appears to have timed the release of its *Ransomware Action Plan* to coincide with the event.

The 16-page plan opens with an address from Karen Andrews, the Minister for Home Affairs, which explains that "[t]his Ransomware Action Plan sets out the Government's immediate strategic approach to tackle the threat posed by ransomware."[6] She goes on to detail how the plan should be seen as building on prior policies like the 2016 and 2020 Cyber Security Strategies, and the National Strategy to Fight Transnational, Serious

and Organised Crime.[7] Lastly, Andrews emphatically states that the Australian government has a "zero tolerance approach to ransomware" and is firmly against any ransom payment being made, regardless of the size.[8]

After contextualizing the threats ransomware can pose, the final five pages get to the meat of the *Ransomware Action Plan*'s three policy objectives and related initiatives. *Prepare and Prevent* focuses on building resilience, *Respond and Recover* concerns improving ransomware victim support, and *Disrupt and Deter* discusses deterrence and disruption through offensive action and by "strengthening Australia's criminal law regime."

Alongside these objectives are several anticipated policy and operational responses, as well as legislative reforms. The most notable of these include:[9]

- Actively calling out those who support, facilitate or provide safe havens to cybercriminals
- Introducing a specific mandatory ransomware incident reporting to the Australian Government
- Introducing a stand-alone offence for all forms of cyber extortion
- Introducing a stand-alone aggravated offence for cybercriminals seeking to target critical infrastructure
- Modernising legislation to ensure that cybercriminals are held to account for their actions, and law enforcement is able to track and seize or freeze their ill-gotten gains

Action & Analysis
Membership Required

3. Cyber Threats Continue to Target U.S. Critical Infrastructure

On October 14th, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) released a joint advisory to highlight "ongoing malicious cyber activity—by both known and unknown actors—targeting the information technology (IT) and operational technology (OT) networks, systems, and devices of U.S. Water and Wastewater Systems (WWS) Sector facilities."[10] The advisory underscores how threats of malicious cyber activity against the United States' critical infrastructure has become increasingly common.

The advisory states that the noted malicious activity "includes attempts to compromise system integrity via unauthorized access" and "threatens the ability of WWS facilities to provide clean, potable water to, and effectively manage the wastewater of, their communities."[11] Concerningly, the advisory also noted three previously unknown ransomware attacks against WWS facilities since March of this year, adding to three other well-known incidents that occurred in 2021.[12]

While the focus of the advisory was on WWS, it acknowledges that cyber threats across other critical infrastructure sectors are increasing. Additional information provided as part of the advisory's threat overview will sound familiar to those in the healthcare sector, as it warns of spearphishing, ransomware, RDP compromise, and insider threats.

Actions & Analysis
Membership Required

Congress

Tuesday, October 19th:
- No relevant hearings

Wednesday, October 20th:
- No relevant hearings

Thursday, October 21st:
- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

October 19th, 2021

Conferences, Webinars, and Summits –

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

---

[1] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

[2] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

[4] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

[5] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

[6] https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

[7] https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

[8] https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

[9] https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf

[10] https://us-cert.cisa.gov/ncas/alerts/aa21-287a

[11] https://us-cert.cisa.gov/ncas/alerts/aa21-287a

[12] https://therecord.media/us-govt-reveals-three-more-ransomware-attacks-on-water-treatment-plants-this-year/