June 22nd, 2021

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins by breaking down President Biden's meeting with Russian President Putin. We examine what was said and agreed to and then assess the likelihood that it will result in improvements in relations and a decrease in malicious cyber activity. Next, we jump into a recent report on the state of ransomware, specifically to the costs to businesses. Finally, we end by highlighting NIST's newest Cybersecurity Framework profile for ransomware risk management and encourage members to evaluate how it may help them respond to the ransomware threat. Welcome back to *Hacking Healthcare*.

1. Biden Confronts Putin on Malicious Cyber Activity

Public and private sector cybersecurity experts across the globe have been pointing out for years that the criminal and state directed cyber operations that appear to emanate from Russia often ignore widely accepted norms of behavior and typically go unpunished. In an effort to address this issue, President Biden made time to specifically bring up malicious cyber activities during last week's face-to-face meeting with Russian President Vladimir Putin.

It has been reported that Biden gave Putin a list of 16 critical infrastructure sectors that should never be targeted by malicious cyber actions. The 16 sectors, outlined in Presidential Policy Directive 21 (PPD-21), include many directly related to healthcare, such as Emergency Services, Healthcare and Public Health, Chemical, Information Technology, and Critical Manufacturing.[1] According to Biden, he made clear to Putin that, "certain critical infrastructure should be off-limits to attack, period, by cyber or any other means."[2]

In addition to critical infrastructure, it was reported that both states had agreed to begin a dialog over "specific understandings about what's off-limits and to follow up on specific [cyber incidents] that originate in either of our countries."[3] This may include coming to a mutual understanding of "cyber aggression red lines."[4]

Action & Analysis
Included with H-ISAC Membership

2. Does Paying a Ransom Invite Further Ransom Attacks?

Determining the best course of action when victimized by ransomware depends in part on an organization's understanding of the current ransomware environment. As cybercriminals modify and adapt their tactics, it's useful to understand these changes and adapt response plans accordingly. Cybereason's release of their *Ransomware: The True Cost to Business* report helps shine a light on the current ransomware threat environment, and some of its findings are particularly illuminating when it comes to the decision to pay or not pay a ransom.

The freely available 31-page report was compiled in April of this year and includes input from 1,263 respondents in the United States, Spain, France, the United Kingdom, Germany, The United Arab Emirates, and Singapore.[5] While technology, manufacturing, and finance sectors are heavily represented, the study also includes healthcare and other industries as well.[6]

Some of the top-level takeaways in Cybereason's report are:[7]

- 80% of respondents that were ransomware victims and paid experienced another attack, and 46% believe that the follow-on attack was committed by the original perpetrator

- 46% of respondents regained access to their data following payment, but some or all of the data was corrupted

- 64% of healthcare respondents reported revenue loss following a successful ransomware attack

- 24% of healthcare respondents reported workforce reductions following a successful ransomware attack

- 53% of respondents said their brand suffered as a result of a ransomware attack – with that number rising to 56% for organizations in the United States

- 42% of respondents said cyber insurance did not cover all their losses.

The report concludes with an emphasis on taking strong, in-depth preventative measures in addition to having robust detection and response capabilities.

Action & Analysis
Included with H-ISAC Membership

3. NIST Releases Preliminary Draft: Cybersecurity Framework Profile for Ransomware Risk Management

On June 9th, the National Institute of Standards and Technology (NIST) released their preliminary draft of NISTIR 8374, the *Cybersecurity Framework Profile for Ransomware Risk Management*. Coming during an onslaught of ransomware activity, the preliminary draft “defines a Ransomware Profile, which identifies security objectives from the NIST Cybersecurity Framework that support preventing, responding to, and recovering from ransomware events.”[8]

As NIST notes, the framework profile “can be used as a guide to managing the risk of ransomware events. That includes helping to gauge an organization's level of readiness to mitigate ransomware threats and to react to the potential impact of events.”[9] While the document itself is written to be generally accessible and useable by anyone, those familiar with the NIST Cybersecurity Framework (CSF) will immediately recognize the formatting. At only 22-pages, the document won’t overload readers and it helpfully includes informative references and additional resources.

The draft is open for comments until July 9th, and those organizations interested should feel encouraged to engage with NIST in the finalization of the document. For those who would like to comment but cannot turn something around in short order, NIST has noted that there will be at least one more public comment period before final publication.

Action & Analysis
Included with H-ISAC Membership

Congress –

<u>Tuesday, June 22nd</u>:
- No relevant hearings

<u>Wednesday, June 23rd</u>:
- Senate – Committee on Armed Services – Subcommittee on Cybersecurity: Hearings to examine recent ransomware attacks

<u>Thursday, June 24th:</u>
- House of Representatives – Committee on Energy and Commerce – Subcommittee on Health: Hearing “Empowered by Data: Legislation to Advance Equity and Public Health”

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits –

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

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

[1] https://www.cisa.gov/critical-infrastructure-sectors
[2] https://www.cyberscoop.com/biden-putin-summit-russia-geneva/

June 22nd, 2021

[3] https://www.cyberscoop.com/biden-putin-summit-russia-geneva/

[4] https://www.cyberscoop.com/biden-putin-summit-russia-geneva/

[5] https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

[6] https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

[7] https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

[8] https://csrc.nist.gov/publications/detail/nistir/8374/draft

[9] https://csrc.nist.gov/publications/detail/nistir/8374/draft