August 17th, 2021

TLP White

This week, *Hacking Healthcare* begins by examining an alarming report that a secret government watchlist may have been left exposed online, raising questions about how concerned companies should be over information sharing and mandatory reporting. Next, we briefly assess an ongoing lawsuit against SolarWinds that's notable because it partially targets their CISO. Finally, we wrap up by breaking down Proofpoint's latest CISO report to glean useful takeaways and noteworthy trends.

Welcome back to *Hacking Healthcare*.

1. **Secret Watchlist Exposure Raises Questions**

   It isn't a secret that governments around the world keep valuable databases and watchlists for all manner of important intelligence tracking and analysis purposes. Given how highly sensitive the information on these lists can be, you would expect the security and privacy controls and policies put in place to keep them out of the public domain to be robust. For that reason, the apparent exposure of some 1.9 million records that appear related to some form of government terrorist/no fly watchlist raises some questions that are applicable to the healthcare sector.

   According to reports, a security researcher happened upon an accessible, passwordless, Elasticsearch cluster that contained 1.9 million records.[1] The records included what appear to be highly sensitive fields such as first and last name, citizenship, gender, date of birth, "no fly indicator," and passport details.[2] Furthermore, the records include a field that appears to be an identifier related to the United States' Terrorist Screening Center (TSC).[3] The TSC is a "multi-agency center administered by the FBI" that "is a single database that contains sensitive national security and law enforcement information concerning the identities of those who are known or reasonably suspected of being involved in terrorist activities."[4]

   The security researcher who stumbled upon this data acted quickly and in good faith to report the issue to the Department of Homeland Security (DHS), but the exposed server

remained online for another three weeks, and it is unknown who else may have accessed it as it was reported that the server had been indexed by at least two search engines.[5] It is also unclear if the list and data are genuine, recent, and who might have been responsible for this particular instance of it surfacing online. As of this writing, neither the Federal Bureau of Investigation (FBI) nor DHS has offered a public statement.

Action & Analysis
Membership required

2. SolarWinds Highlights Legal Risk to C-Suite

In the aftermath of the SolarWinds incident, it has been reported that a group of investors filed a suit that "claims that inaction around cybersecurity led to deception for investors," and it includes naming the company's former CEO and CISO directly.[6]

According to SecureWorld, the lawsuit claims that SolarWinds had abysmal security practices and leadership, and that it made "misleading claims about the quality of its cybersecurity."[7] The suit itself going as far to say that "[t]here was no security team, there was no password policy, there was no documentation regarding data protection and controls, and the Company did not limit user access controls."[8] Some of these claims have apparently been supported by former employees, but SolarWinds has since pushed back on this narrative.

In their response, SolarWinds defended their security measures and rejected the notion that either their CEO or CISO was at fault. They emphasized that the general consensus surrounding the incident suggested that it was unreasonable to expect a singular entity to be able to deter an attack of this sophistication. It may be some time before this lawsuit plays out to completion.

Action & Analysis
Membership required

3. Proofpoint's CISO Report

It is always helpful for CISOs to be able to understand their work in the larger context of what's going on in the world. Knowing the challenges, solutions, and priorities of other CISOs helps provide a frame of reference and can be useful in having conversations with organizational leadership. With that in mind, we felt that a quick breakdown of Proofpoint's most recent *Voice of the CISO Report* would be worthwhile.

The 17-page report catalogs one of the more unique and challenging years CISOs have faced. The report is based off a survey of 1,400 CISOs from across the globe and it

tackles a number of important topics ranging from "facing a dynamic threat landscape," to hybrid working, and CISO satisfaction, challenges, and expectations.[9]

The results are illuminating, and some of the more interesting ones include:[10]

- Globally, 64% of CISOs agree their organization is at risk of a material cyberattack in the next 12 months.
- The public sector is far more optimistic that attacks on their organizations will not result in material damage.
- Despite ransomware's headline grabbing, it ranks 7th in biggest perceived risk (27%) among CISOs, behind Business Email Compromises (BEC) (34%), Cloud Account Compromise (33%), Insider threat (31%), DDoS (30%), Supply Chain Attack (29%), and Cyber/Physical (28%).
- 58% of CISOs globally think their employees understand their role in protecting their organization from cyberattacks. That number rises above 70% in Japan and Germany and to 62% in the United States.
- 75% of CISOs based in the United States believe that human error is their organization's biggest cyber vulnerability.
- Interestingly, CISOs appear to find increasing levels of support from their organizations' boards of directors as the size of an organization increases. This jumps from 54% agreeing their perspectives are aligned with boards at organizations of 501-1000 employees to 71% at organizations over 5,001 employees.

The full report is freely available online and contains much more data and statistics for members to comb through.

Action & Analysis
Membership required

Congress –

<u>Tuesday, August 17th</u>:
- No relevant hearings

<u>Wednesday, August 18th</u>:
- No relevant hearings

<u>Thursday, August 19th:</u>

August 17th, 2021

- No relevant hearings

International Hearings/Meetings –
- No relevant meetings

EU –

Conferences, Webinars, and Summits –

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

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

---

[1] https://www.bleepingcomputer.com/news/security/secret-terrorist-watchlist-with-2-million-records-exposed-online/
[2] https://www.bleepingcomputer.com/news/security/secret-terrorist-watchlist-with-2-million-records-exposed-online/
[3] https://www.bleepingcomputer.com/news/security/secret-terrorist-watchlist-with-2-million-records-exposed-online/
[4] https://www.fbi.gov/about/leadership-and-structure/national-security-branch/tsc
[5] https://www.bleepingcomputer.com/news/security/secret-terrorist-watchlist-with-2-million-records-exposed-online/
[6] https://www.secureworld.io/industry-news/ciso-lawsuit-solarwinds
[7] https://www.secureworld.io/industry-news/ciso-lawsuit-solarwinds
[8] https://www.secureworld.io/industry-news/ciso-lawsuit-solarwinds
[9] https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-voice-of-the-CISO-report.pdf
[10] https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-voice-of-the-CISO-report.pdf