EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

The Equifax Hack Revisited and Repurposed

Hal Berghel, University of Nevada, Las Vegas

The recent indictments against Chinese hackers should be seen as political theater. Once again, the Equifax hack rears its ugly head—but this time for a political purpose.

BACKGROUND

There has never been any serious dispute over the nature of the Equifax hack and not much dispute over the perpetrators. *Bloomberg Businessweek* speculated shortly after the hack was announced in 2017 that it was likely state sponsored,[1] and the *Daily Mail* expanded the speculation by accusing China the next day.[2] Although Barr gives the impression that the China connection was discovered only through a no-stone-unturned crackerjack investigation by his office, in fact, his office's announcement was three years late to the party. The announcement is a rather pedestrian attempt to keep the story alive for reasons that have nothing to do with the crime or injury to victims.

On 10 February 2020, U.S. Attorney General William Barr announced the indictment of four Chinese military personnel for hacking into the Equifax servers in 2017 (https://www.youtube.com/watch?v=IpEuUzMPpxI). To the uninitiated, the presentation may impart minimal confidence in the U.S. Department of Justice (DoJ), but to nonpartisan security specialists, it will be seen as a purposeless effort to draw attention away from other topics, such as the real problems underscored by the Equifax hack and the recent questionable behavior by the DoJ. Barr's anticlimactic faux prosecution announcement is taken from the pages of Aldous Huxley and George Orwell. It falls under the rubric of what I call *juridical superfluity*. Allow me to explain why I say this.

What we know for certain is that Barr and the DoJ decided to actually prosecute four members of the Chinese People's Liberation Army.[3] Of course, the likelihood that these individuals will be arrested, much less prosecuted and convicted, is about as likely as Donald Trump willingly providing his tax returns to the *Washington Post*. Good luck on serving those arrest warrants. As I've written before in this column, state-sponsored hacks are not uncommon these days. But as Andy Greenberg has noted, such pointless prosecutions may lead to a tit-for-tat retaliation

Digital Object Identifier 10.1109/MC.2020.2979525
Date of current version: 7 May 2020

by those targeted.[4] Hopefully, savvy journalists and the public will come to understand Barr's Sinophobic rant for the political hokum that it is. However, Barr is the attorney general, so his announcement deserves some careful analysis.

The actual indictment[5] is historically, if not judicially, interesting. It reports that "on or about 13 2018 May and continuing through on or about 30 July 2017 members of the People's Liberation Army ... conspired with each other to hack into the protected computers of Equifax ... to steal sensitive personally identifiable information of 145 million Americans." The hack took place through the unpatched Apache Struts Server maintained by Equifax. Although the patch for this vulnerability was announced on 7 March 2017,[6] the Equifax IT security team, led by a chief information security officer (CISO) with a background in music composition,[10,11] didn't bother to apply it. In fact, Equifax didn't even announce the hack to the public until early September, six weeks after the incident.[8] The fact that hackers accessed the personally identifiable information (PII) of half the U.S. population through a known, yet unpatched, security vulnerability falls under the rubric of what I label *corporate faith-based security*.[9]

No purposeless indictment would be complete without primitive visual aids, and this one does not disappoint. Photos of three of the four accused in military uniforms are appended. One may only assume that the gratuitous addition of photos to an indictment is intended to provide a dash of extra credibility to an otherwise feckless, but formal, legal document. Does anyone expect the photos to be prominently displayed on kiosks in theme parks and post offices coast to coast? Photos attached to indictments relating to national security offers a new step into future prosecutorial propaganda. I, for one, just can't wait until the DoJ starts making national security indictments a staple on YouTube, the online equivalent of *Judge Judy* for the national security complex. By way of comparison, one might look to the indictment of the 12 Russian intelligence officers for interfering with the 2016 U.S. presidential election,[12] no gratuitous media to be found anywhere therein. Could it be that Barr's DoJ has an entirely different agenda in the Chinese Equifax case?

Well wonder no more because it becomes clear in Section 5.b. of the indictment. We are informed that Equifax has taken "reasonable measures to keep [their trade secrets] secret ... " from others who might seek to exploit their economic value. Just what were these reasonable measures? To answer that, we need to turn to the U.S. Senate report of the incident, which came out in early 2019.[13]

The Senate consensus follows immediately from the title of the Senate report "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach." We note the difference between the tone of the Senate report and Barr's indictment. What Barr considers "reasonable measures" was deemed "neglected cybersecurity" by the Senate. But it gets worse for Equifax and the indictment hokum as one digs into the report. According to the report,

- Equifax learned of significant cybersecurity deficiencies in 2015, two years before the alleged Chinese hack. "[A] 2015 security audit identified more than 8,500 vulnerabilities that Equifax employees failed to address for more than 90 days beyond the recommended patching timeframe," 1,000 of which were rated as critical, high, or medium.
- Equifax lacked a comprehensive IT asset inventory; specifically, it didn't know whether it was using the Apache Struts software so it wasn't aware of the need to patch it.
- Equifax used what internal auditors called *an honor system* for patching vulnerabilities, that is, it had no formal method for validating the successful installation of patches.
- Equifax did not employ follow-up audits after the 2015 one to determine whether the vulnerabilities remained.
- The CISO did not regularly attend the "global threats and vulnerability management" meetings where security vulnerabilities (like Apache Struts) were discussed, and Equifax had no policy regarding mandatory attendance.
- Equifax networked systems were not isolated. The hackers entered the IT infrastructure through Equifax's Online Dispute Portal and through that accessed other sensitive and unencrypted databases.
- Equifax failed to adequately enforce SSL certificate management policies.
- Equifax's records retention policy did not include all relevant incident response records, as they used instant messaging as their primary communication medium, and these communications were considered ephemeral and not retained.

This is just a partial list of Equifax's security deficiencies, but based on Barr's announcement, they qualify as "reasonable measures" to protect sensitive data. We won't even mention that Equifax had no formal policy on the disclosure of compromised customer information—it waited six weeks to make the public announcement that they had been hacked. Careful reading of the Senate report suggests that the Equifax hack was less of a hack than an illegal intrusion. What Equifax did was create an attractive cybernuisance.

Of course, the Equifax postmortem shows that the staff, for the most part, assumed a cover-your-assets (CYA) stance. To paraphrase, no one could

have prevented this, as it was the most sophisticated cyberattack imaginable and totally indefensible—yadda, yadda, yadda. Such claims are typical of embarrassed organizations and should be taken with the proverbial pinch of salt. Equifax didn't know what assets it had nor what was needed to protect them; the CISO didn't attend the vulnerability management meetings; disparate components of the networked infrastructure weren't properly isolated; it didn't bother to implement certificate management policies; inadequate attention was paid to egress traffic and the customer data wasn't adequately encrypted—then the Chinese stole it. Who could've seen that coming, according to Barr. As I've mentioned before,[14] in many ways, these CYA tactics and lame excuses resemble Elisabeth Kubler-Ross's five stages of grief. Equifax had a proven track record of ineptitude when it came to IT security controls and the protection of the data it held. Equifax security policy—and I use this term reluctantly—is analogous to locking your doors but leaving a few windows open. From an IT security point of view, none of this qualifies as a reasonable measure to protect sensitive data.

Ultimately, the standard barometer for determining the adequacy of security systems is whether they conform to industry best practices. There is no silver bullet to be found. If all of the competition adopts the same or similar information security policy, at least your organization can't be singled out as the lone incompetent player. As it turns out, the Senate report deals with this aspect as well by comparing Equifax's security practices, especially patch policies, with those of TransUnion and Experian, Equifax's closest business competitors. It should come as no surprise that Equifax suffers for the comparison in many ways and at most levels, specifically including ameliorating the Apache Struts vulnerability. It's all to be found in the Senate report and postmortems by security specialists.[15]

THE REST OF THE STORY

The Senate findings make the DoJ's indictment all the more curious. Without belaboring the point, a thorough understanding of the Equifax hack naturally suggests the following questions:

- Why does the indictment's analysis of the hack downplay Equifax's culpability? The indictment seems to suggest that the four accused were supergeeks who blazed a path to as-yet-unimagined hacker triumphs. But the evidence shows that they were primarily exploiting a known vulnerability that one of the credit-reporting companies (namely, Equifax) simply chose to ignore. The facts suggest that far from cutting-edge cyberaggression, the Equifax hack was more of an exercise in Hacking 101.
- Given the Senate report (and other responsible accounts from the technical press[16–20]), how could Barr and the DoJ expect their defense of Equifax's cybersecurity practices to be taken seriously? If industry best practices are to be our guide, there was nothing reasonable about it—amateurish seems to be a better fit. The wording in the indictment suggests that the purpose of the indictment is more theatrical than legal.
- Why is the emphasis in the indictment on the harm done to Equifax (and their world-class business practices) rather than that done to Equifax's innocent customers whose compromised PII will doubtless lead to decades of future identity theft problems?
- What accounts for the timing of this seemingly senseless indictment? Temporally, we know that Barr's press release was the day before he overturned his prosecutor's sentencing recommendation for Roger Stone and a few days before President Trump went on his latest pardon spree that included Michael Milken, Bernard Kerik, and Rod Blagojevich. The coincidence cannot be overlooked. If the indictment were intuitively justified and made a lot of legal sense, one might be tempted to ignore the coincidence. But in this case, especially given the history of the principals involved, the indictment doesn't pass my smell test. The possibility of a sleight-of-hand move to distract public attention from attendant thorny political issues seems a likely possibility.
- Finally, one has to ask of all the bad actors: Which are the most dangerous to the United States and its citizens? Foreign hackers or incompetent corporations who fail to respect the privacy and PII of their customers' data? There is no question that Equifax has not proven itself to be a responsible steward of the public's PII. The total penalty to date, even if we take the higher figure, will serve as no deterrent to future irresponsible corporate behavior. Quite the contrary, it provides just one more moral hazard.

I encourage digital security specialists and investigators to repeat my analysis and derive their own conclusions. Incidentally, irresponsible behavior is not limited to Equifax's chief information officer and CISO. According to an indictment by the U.S. District Court for the Northern District of Georgia,[21] after becoming aware of the hack, Sudhakar Bonthu, former Equifax production development manager of software engineering in Equifax' global consumer services division, bought US$2,166 worth of out-of-the-money put option contracts for shares of Equifax common stock on 1 September 2017 in anticipation

of Equifax's disclosure of the breach. The common stock dropped 14% on 8 September 2017, the day following the announcement, whereupon Bonthu exercised his options, profiting by US$75,168—a return of 3,500% in six days for his 86 put options. Because Bonthu's trading was based on material nonpublic information entrusted to him by Equifax, the U.S. District Court demanded that he forfeit the money with interest, pay a fine of US$50,000, and serve eight months of home confinement.[22]

Equally interesting to me is that two days after the intrusion was discovered by Equifax, the U.S. Securities and Exchange Commission's records confirmed that three Equifax executives (the chief financial officer, workforce solutions president, and U.S. information solutions president) sold approximately US$2 million in Equifax stock from their portfolios.[23,24] Coincidence? To top that, Rick Smith, the chief executive officer of Equifax at the time of the hack, was subsequently given a US$90 million retirement package.[25] This is the stuff of which dime store novels on crony capitalism are made. There is definitely a Quentin Tarantino movie in this somewhere. I propose the following modest titles: *Data Dogs* or *Once Upon a Time with Identity Theft*.

So, what was the ultimate cost to Equifax? The actual settlement was somewhere between US$700 million and US$1.4 billion, depending on how and what you count.[26,27] However, by all accounts, the amount available for victim reparations is US$425 million,[28] and approximately US$80 million is provided for attorney's fees, with some additional amounts for fines and penalties (https://www.youtube.com/watch?v=9GZQ1Nh_Rj8). That's right, US$3 per victim for reparations! The paltry amount allocated to victim indemnification guarantees that, on average, the victims' financial damage will remain uncompensated. But what is worse is that there is an onerous requirement that victims "prove up" any claimed losses. Proving up requires not only that the victims document damage but that they also prove that the damage directly resulted from the Equifax incident and cannot have been the result of any other incident or action—an impossible challenge for any individual not currently a member of the country club set. Not surprisingly, I have a suggestion. Because Barr is already in "gratuitous prosecution" mode, I think it only reasonable that he should sue the Chinese government for US$150 trillion for victim reparations (that's US$100,000 per victim that, in my opinion, is far more realistic than the US$3 that the Federal Trade Commission seeks from Equifax). Of course, that suit would go nowhere either, but it might provide the victims with more consolation than the futile prosecutions of four Chinese soldiers. If nothing else is accomplished, it offers better judicial theatrics.

One final thought on how the world might move forward purposefully from the Equifax experience. The Council of Europe adopted its Convention on Cybercrime (also known as the Budapest Convention) in 2001.[29] This convention, and its 2006 extension, mandates that signatory countries pass laws that recognize and prosecute cybercrimes, broadly defined. Specifically, enumerated crimes include the illegal access to and use of computing systems and networks, computer-related fraud, violations of copyright, offenses involving child pornography, hate crimes, the distribution of racist material, and so on. As of 3 February 2020, most of the members of the Council of Europe (except Russia) have signed the Budapest Convention, and only Sweden and Ireland have failed to ratify. The United States and its non-European allies have mostly ratified as well (notable exceptions include Mexico, Brazil, China, and India).[30] In 2019, the United Nations (UN) began debate of a similar treaty initiated by Russia that included contributions from China, Australia, Canada, Cuba, the United Kingdom, Japan, and several other allies.[31] I'm sure you can see where this is headed. Because the initiative was inspired by Russia and China, western corporatists and American exceptionalists are unenthusiastic.

The issue is national sovereignty and corporate interests. The U.S. position has always been strongly myopic, defending against any international judicial effort that might undermine inviolability of U.S. interests. The United States also took this stance 10 years ago when it opposed a similar U.N. treaty on cybercrime.[32] What the United States does not want is any international policy that interferes with existing U.S. monopolies in cyberspace and high tech, injects itself into any future tech space that the United States has carved out for itself, extends international investigatory reach into protected corporate space, undercuts the evidentiary standards currently applied by U.S. courts, and so on. This posture is a consequence of the same American exceptionalism that led to the refusal of the United States to support the International Criminal Court and prompted the 2002 passage of the Hague Invasion Act. The U.S. demand that it be immune to accountability suggests that a more accurate term might be *American exemptionalism*. As long as such nationalistic attitudes prevail, it will be difficult to get all prospective international criminals to unite behind cybercriminal activity, and a consequence of this will be that the United States will remain an attractive target.

REFERENCES

1. M. Riley, J. Robertson, and A. Sharpe, "The Equifax hack has the hallmarks of state-sponsored pros," *Bloomberg Businessweek*, Sept. 29, 2017. [Online]. Available: https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros

2. K. Griffith, "Was it China? Clues point to state sponsorship of massive Equifax hack," *Mail Online*, Sept. 30, 2017. [Online]. Available: https://www.dailymail.co.uk/news/article-4937010/Clues-suggest-China-suspect-massive-Equifax-hack.html
3. "Chinese military personnel charged with computer fraud, economic espionage and wire fraud for hacking into Credit Reporting Agency Equifax," Department of Justice, Office of Public Affairs, Washington, D.C., Feb. 10, 2020. [Online]. Available: https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking
4. A. Greenberg, "U.S. indictment of Chinese hackers could be awkward for the NSA," *Wired*, May 19, 2014. Accessed on: Feb. 11, 2020. [Online]. Available: https://www.wired.com/2014/05/us-indictments-of-chinese-military-hackers-could-be-awkward-for-nsa/
5. U.S. v. W. Zhiyong, W. Qian, X. Ke, and L. Lei, Criminal Indictment No. 2:20-CD046, U.S. District Court for the Northern District of Georgia Atlanta Division, Jan. 28, 2020. [Online]. Available: https://www.justice.gov/opa/press-release/file/1246891/download
6. "The Apache Software Foundation confirms Equifax data breach due to failure to install patches provided for Apache Struts exploit," Apache Software Foundation, Sept. 14, 2017. [Online]. Available: https://blogs.apache.org/foundation/entry/media-alert-the-apache-software
7. "Critical patch for Apache Struts server, re: CVE-2017-5638," Security Bulletin S2-045, Apache Software Foundation, last revised Mar. 19, 2017. [Online]. Available: https://cwiki.apache.org/confluence/display/WW/S2-045
8. L. H. Newman, "All the ways Equifax epically bungled its breach response," *Wired*, Sept. 9, 2017. [Online]. Available: https://www.wired.com/story/equifax-breach-response/
9. H. Berghel, "Faith-based security," *Commun. ACM*, vol. 51, no. 4, pp. 13–17, Apr. 2008. doi: 10.1145/1330311.1330315. [Online]. Available: https://cacm.acm.org/magazines/2008/4/5432-faith-based-security/fulltext
10. B. Arends, "Equifax hired a music major as chief security officer and she has just retired," MarketWatch, Sept. 15, 2017. [Online]. Available: https://www.marketwatch.com/story/equifax-ceo-hired-a-music-major-as-the-companys-chief-security-officer-2017-09-15
11. K. Sweet, "Key Equifax executives departing after huge data breach," Associated Press, Sept. 17, 2017. [Online]. Available: https://apnews.com/68e36912eb4047dbbb532192e6648479
12. U.S. v. V. B. Netyksho et al., Case 1:18-cr-00215-ABJ, U.S. District Court for the District of Columbia, Washington, D.C., July 13, 2018. [Online]. Available: https://www.justice.gov/file/1080281/download
13. "How Equifax neglected cybersecurity and suffered a devastating data breach," Staff Rep. (final), Permanent Subcommittee on Investigations, U.S. Senate, Washington, D.C., Mar. 2019. [Online]. Available: https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf
14. H. Berghel, "The SCDOR hack: Great security theater in five stages," *Computer*, vol. 46, no. 3, pp. 91–93, Mar. 2013. doi: 10.1109/MC.2013.117. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6489958
15. L. Spitzner, "The congressional report on Equifax hack," SANS Security Awareness Website, Dec. 2018. [Online]. Available: https://www.sans.org/security-awareness-training/blog/just-released-congressional-report-equifax-hack
16. J. Sowells, "Equifax's senate investigation: What went wrong?" Hacker Combat, Mar. 9, 2019. [Online]. Available:
17. M. Dove, "Equifax: Senate goes once more into the breach," *The Fintech Times*, Mar. 26, 2019. [Online]. Available: https://thefintechtimes.com/equifax-breach-senate/
18. A. Shepherd, "The Equifax Effect: Explaining the biggest security disaster in the 21st century," ITPRO, 15 Mar, 2019. [Online]. Available: https://www.itpro.co.uk/security/33242/the-equifax-effect-explaining-the-biggest-security-disaster-of-the-21st-century
19. L. H. Newman, "The Wired guide to data breaches," *Wired*, July 12, 2018. [Online]. Available: https://www.wired.com/story/wired-guide-to-data-breaches/
20. B. Krebs, "Ayuds! (help!) Equifax has my data!" *Krebs on Security*, Sept. 17, 2020. [Online]. Available: https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/
21. Securities and Exchange Commission v. S. R. Bonthu, Case 1:18-cv-03114-MLB, U.S. District Court for the Northern District of Georgia Atlanta Division, Atlanta, GA, June 28, 2018. Accessed on: Feb. 11, 2020. [Online]. Available: https://www.sec.gov/litigation/complaints/2018/comp-pr2018-115.pdf
22. "Former Equifax manager sentenced for insider trading," Department of Justice, U.S. Attorney's Office, Northern District of Georgia, Atlanta, GA, Oct. 16, 2018. Accessed on: Feb. 11, 2020. [Online]. Available: https://www.justice.gov/usao-ndga/pr/former-equifax-manager-sentenced-insider-trading
23. T. Haselton and Y. N. Lee, "Three Equifax executives sold $2 million worth of shares days after cyberattack," *CNBC Tech*, Sept. 7, 2017. [Online]. Available: https://www.cnbc.com/2017/09/07/equifax-cyberattack-three-executives-sold-shares-worth-nearly-2-million-days-after-data-breach.html
24. T. Loughran, "Equifax President who sold EFX stock on 8/1," *Hollywood LA News*, Sept. 10, 2017. [Online]. Available: https://www.hollywoodlanews.com/joseph-trey-loughran-equifax/

25. J. Wieczner, "Equifax CEO Richard Smith who oversaw breach to collect $90 million," *Fortune*, Sept. 26, 2017. [Online]. Available: https://fortune.com/2017/09/26/equifax-ceo-richard-smith-net-worth/
26. A. St. John, "Equifax settlement: What's in it for consumers," *Consumer Reports*, July 22, 2019. [Online]. Available: https://www.consumerreports.org/credit-bureaus/equifax-settlement/
27. R. McDonald, "Equifax reaches $1.4B data breach settlement in consumer class Action," LAW.COM, July 22, 2019. [Online]. Available: https://www.law.com/nationallawjournal/2019/07/22/equifax-reaches-1-4-billion-data-breach-settlement-in-consumer-class-action/?slreturn=20200202141322
28. "Equifax data breach settlement," Federal Trade Commission, Washington, D.C., Jan. 2020. [Online]. Available: https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
29. "Budapest convention on cybercrime," Council of Europe, Treaty No. 185, 2001. [Online]. Available: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561
30. "Chart of signatures and ratifications of Treaty 185," Council of Europe, Mar. 2, 2020. [Online]. Available: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=lm4tVBVh
31. "Notes from the Open-Ended Working Group 73/27 [on Cybersecurity]," United Nations, Dec. 2019. [Online]. Available: https://www.un.org/disarmament/open-ended-working-group/
32. G. Masters, "Global cybercrime treaty rejected at U.N.," *SC Magazine*, Apr. 23, 2010. [Online]. Available: https://www.scmagazine.com/home/security-news/global-cybercrime-treaty-rejected-at-u-n/

HAL BERGHEL is a Fellow of the IEEE and ACM and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.

Digital Object Identifier 10.1109/MC.2020.2987519