Supplementary Material

I. Processing Using the Medical Text Indexer (MTI)

We sent each of our optical character recognition-processed text files to the MTI and recorded which summaries were classified as being related to software In the MeSH® Tree (ontology). We flagged all products whose summaries were assigned to the "software" MeSH® term, number L01.224.900.

II. Sensitivity Analysis

In sensitivity analyses we considered an alternate method of identifying devices containing software. For this exercise, we electronically scanned each product summary for the keyword "software" and recorded whether the word "software" appeared anywhere within a device's product summary (i.e. at least once in the document).

We expected that the MTI-driven method of identifying the "software sample" would have a high sensitivity but a lower specificity relative to the keyword-based method for the following reason: in order for a text document to be flagged by the MTI's algorithm as being related to the subject of "software" the text document would need describe relevant software content in some detail – i.e. often beyond simply utilizing the keyword "software" at least once.

Indeed, the keyword-based method of identifying software products captured 100% of the products that were identified as including software using the MTI results, but also identified additional products that employ the word "software" in their product summaries at least once (**Supplementary Table**).

Relative to the keyword method, we conclude that the MTI-based method of identifying software products had a 100% sensitivity, but only a 94.8% specificity in our sample. Given the high sensitivity of this method, the MTI-based software sample is the more conservative method for identifying devices with software. However, alternative results using the keyword-based definition are highly similar to those obtained using the MTI-based definition. The total share of the software device sample that includes cybersecurity content is statistically indistinguishable in every year of the sample and visibly similar over time (**Supplementary Table and Supplementary Figure**)

Supplementary Table 1: Comparison of MTI and Keyword-based Methods of Identifying Software over Time

Year	Total Devices	Software sample (MTI defined)	Software sample (keyword defined)	Total devices with cybersecurity content (MTI)	% with cybersecurity content (MTI sample)	Total devices with cybersecurity content (keyword sample)	% with cybersecurity content (keyword)
2002	2573	275	318	3	1.09%	3	0.94%
2003	2565	289	347	3	1.04%	4	1.15%
2004	2476	298	350	4	1.34%	4	1.14%
2005	2338	277	323	2	0.72%	3	0.93%
2006	2430	339	397	5	1.47%	5	1.26%
2007	2245	276	314	8	2.90%	8	2.55%
2008	2333	309	371	6	1.94%	8	2.16%
2009	2287	303	373	3	0.99%	3	0.80%
2010	2168	254	356	2	0.79%	5	1.40%
2011	2405	380	524	6	1.58%	7	1.34%
2012	2466	357	526	3	0.84%	6	1.14%
2013	2404	395	597	11	2.78%	15	2.51%
2014	2509	421	635	7	1.66%	17	2.68%
2015	2334	361	636	20	5.54%	33	5.19%
2016	2261	402	721	22	5.47%	43	5.96%
Totals	35794	4936	6788	105	2.13%	164	2.42%

Supplementary Table 2: List of keywords related to cybersecurity content:

Source	Term	Allowable alternative(s)	Counts
NICCS	access control		17
NICCS	active attack		0
NICCS	air gap		5
NICCS	antispyware software	anti-spyware software, anti-spyware, antispyware	1
NICCS	antivirus software	anti-virus software, anti-virus, antivirus	3
NICCS	asymmetric cryptography		0
NICCS	cipher		0
NICCS	computer network defense		0
NICCS	computer security incident		0
NICCS	cryptanalysis		0
NICCS	cryptographic algorithm		0
NICCS	cryptography		1
NICCS	cyber ecosystem		0
NICCS	cyber exercise		0
NICCS	cyber incident	cyber-incident	0
NICCS	cyber infrastructure	cyber-infrastructure	0
NICCS	cybersecurity	cyber-security	58
NICCS	data breach		0
NICCS	data leakage		0
NICCS	data theft	data-theft	0
NICCS	decrypt		3
NICCS	denial of service	denial-of-service	0
NICCS	designed-in security	designed in security	0
NICCS	digital forensics		0
NICCS	distributed denial of service	distributed denial-of-service, DDOS, D.D.O.S.	0
NICCS	dynamic attack surface		0

NICCS	encrypt		44
NICCS	enterprise risk management		0
NICCS	exploitation analysis		0
NICCS	identity and access management		0
NICCS	information security policy		0
NICCS	information system resilience	Information Systems Security	0
NICCS	Information Systems Security Operations		0
NICCS	intrusion detection		0
NICCS	malicious code		0
NICCS	malware		0
NICCS	NICCS	National Initiative for Cybersecurity Careers and Study	0
NICCS	penetration testing		83
NICCS	phishing		0
NICCS	security incident		0
NICCS	security policy		0
NICCS	spyware	spy-ware	0
NICCS	symmetric cryptography		0
NICCS	symmetric encryption algorithm		0
NICCS	symmetric key		0
NICCS	systems security architecture		0
NICCS	threat assessment		0
FDA Guidance	cybersecurity routine updates and patches	cybersecurity routine updates, cybersecurity routine patches	0
FDA Guidance	cybersecurity signal		0
FDA Guidance	exploit		2
FDA Guidance	Information Sharing Analysis Organizations	ISAO, ISAOs	2
FDA Guidance	NIST	National Institute of Standards and Technology	150
FDA Guidance	NIST Framework	NIST Framework for Improving Critical Infrastructure Cybersecurity	0

Supplementary Figure 1: FDA medical device approval pathways

	Regulatory Pathways for Medical Devices in the United States	
Pathway	510(k) (Premarket Notification)	PMA (Premarket Approval)
Products	Typically moderate-risk ("class II") devices	Typically high-risk ("class III") devices
Requirements	Typically do not necessitate full clinical trials, but require evidence of "substantial equivalence" to a predicate device	Typically require clinical trials to demonstrate a new device's safety and effectiveness
Product develompent time to market	31 months	54 months

Sources:

Maisel WH. Medical device regulation: an introduction for the practicing physician. Annals of internal medicine. 2004 Feb 17;140(4):296-302.

https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k

https://www.fda.gov/medicaldevices/deviceregulationandguidance/howtomarketyourdevice/premarketsubmissions/premarketapprovalpma

Makower J, Meer A, Denend L. FDA impact on US medical technology innovation: a survey of over 200 medical technology companies. Advanced Medical Technology Association, Washington, DC, available at: http://www. advamed. org/NR/rdonlyres/040E6C33-380B-4F6B-AB58-9AB1C0A7A3CF/0/makowerreportfinal. pdf. 2010 Nov.

Supplementary Figure 2: comparison of main results using alternative method of identifying the software sample