CAROLYN B. MALONEY
CHAIRWOMAN

ONE HUNDRED SIXTEENTH CONGRESS

JIM JORDAN, OHIO
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5051
MINORITY (202) 225–5074

http://oversight.house.gov

March 23, 2021

Mr. Brad Smith
President
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Dear Mr. Smith:

Enclosed are questions that have been directed to you and submitted for the official record for the hearing on Friday, February 26, 2021, titled "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign."

Please return your written responses to these questions by Tuesday, April 6, 2021, including each question in full as well as the name of the Member. Your response should be addressed to the Committee office at 2157 Rayburn House Office Building, Washington, D.C. 20515. Please also send an electronic version of your response by email to Amy Stratton, Deputy Chief Clerk, at Amy.Stratton@mail.house.gov.

Thank you for your prompt attention to this request. If you need additional information or have other questions, please contact Elisa LaNier, Chief Clerk, at (202) 225-5051.

Sincerely,

Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform

Enclosure

cc: The Honorable James R. Comer, Ranking Member
Committee on Oversight and Reform

Questions for Brad Smith, President and Chief Legal Officer, Microsoft Corporation

Questions from Chairwoman Carolyn B. Maloney, Committee on Oversight and Reform

February 26, 2021, Hearing: "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign"

---

1. Is Microsoft obligated to monitor for anomalous traffic and suspicious behavior in the Office365 environment and notify its customers if it notices an indication of malicious activity? Please identify any differing levels of monitoring available by contract.

2. We understand that customers of Microsoft and victims of this breach may not have been able to view the communications between the Microsoft cloud server and external servers associated with the malicious activity, but that Microsoft is in a position to see that traffic. For example, during testimony, Mr. Smith stated that "[o]nce [the attackers gained access to the victim's cloud services], we were able to see them because we scan the services that we run every day with a specific eye towards some particular threats." Has Microsoft received any requests for assistance in monitoring from government customers? Please identify which government agencies or components have made such a request.

3. Please provide a breakdown of the specific logging you provide to the following federal agencies and departments for the Office365 environment:

    a. Department of Commerce,
    b. Department of Energy,
    c. Federal Aviation Administration,
    d. Department of Health and Human Services,
    e. Department of Homeland Security,
    f. Department of Justice,
    g. National Aeronautics and Space Administration,
    h. Department of State, and
    i. Department of the Treasury.

4. Please provide an overview of the range of logging Microsoft provides to federal customers under the various licenses, such as G3 and G5. Please identify the least and most amount of logging that you performed under these licenses, and identify the cost difference between the licenses.

5. During the hearing, Mr. Smith stated that "it is a fairly standard aspect of Federal contracting practices that agencies restrict a company, like Microsoft, from sharing with others in the Federal Government when a particular agency has been hacked in this way." Please provide

examples of contractual provisions that prevent Microsoft from being able to share breach information.

6. Please provide a breakdown of your expected costs associated with this breach.

Brad Smith
President and Chief Legal Officer
Microsoft Corporation

February 26, 2021, Hearing: "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign"

Questions from Rep. Jim Cooper

During the House Committee on Oversight and Reform hearing on February 26, 2021, on the role of your companies in the "SolarWinds breach," I asked each of you about your company's errors and omissions insurance. Only Mr. Smith said that Microsoft was self-insured.

In SolarWinds' IPO Prospectus from 2018, SolarWinds stated, "[d]espite our security measures, unauthorized access to, or security breaches of, our software or systems could result in the loss, compromise or corruption of data, loss of business, severe reputational damage adversely affecting customer or investor confidence, regulatory investigations and orders, litigation, indemnity obligations, damages for contract breach, penalties for violation of applicable laws or regulations, significant costs for remediation and other liabilities." SolarWinds continued, "… [o]ur errors and omissions insurance coverage covering certain security and privacy damages and claim expenses may not be sufficient to compensate for all liabilities we incur."

As SolarWinds warned investors, E&O insurance could help protect the company from hacks or attacks, but might not be able to do so completely, and such coverage does nothing for your customers. There are several ways that insurance could affect your company: 1) it protects you, not your customers, so it is not necessarily aligned with your customers' interests; 2) it creates a moral hazard for your company that diminishes your interest in securing your own software, particularly if your insurance coverage is extensive; and 3) it means that future premium increases could increase your company's attention on securing your software from hacks.

When I asked each of you for information regarding your insurance coverage related to security breaches, you stated that you would need to find the answers and submit them for the record. Again, I am asking you each the following questions:

1. If your company has errors and omissions insurance coverage for damages incurred from security breaches, or other cyber liability insurance for costs related to security breaches, please provide:

    a. What claims is your company making to your insurers related to the SolarWinds breach?

b. How much money was paid, or is expected to be paid, by your insurers for these claims?

c. Since filing these claims, will your insurance premiums increase, or do you expect them to increase? If so, by how much?

2. Which insurance companies provide your errors and omission insurance, or other insurance related to security breaches? If you are self-insured, is there an internal mechanism in your company that serves the same function?

3. What are the major insurance companies that provide this coverage to your industry?

4. What percentage of your industry has this coverage? To your knowledge, do your competitors have this coverage?

Responding to Oversight Committee Document Requests

1. In complying with this request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. Produce all documents that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party.

2. Requested documents, and all documents reasonably related to the requested documents, should not be destroyed, altered, removed, transferred, or otherwise made inaccessible to the Committee.

3. In the event that any entity, organization, or individual denoted in this request is or has been known by any name other than that herein denoted, the request shall be read also to include that alternative identification.

4. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, thumb drive, or secure file transfer) in lieu of paper productions.

5. Documents produced in electronic format should be organized, identified, and indexed electronically.

6. Electronic document productions should be prepared according to the following standards:

    a. The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.

    b. Document numbers in the load file should match document Bates numbers and TIF file names.

    c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.

    d. All electronic documents produced to the Committee should include the following fields of metadata specific to each document, and no modifications should be made to the original metadata:

        BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,

INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION, BEGATTACH.

7. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, zip file, box, or folder is produced, each should contain an index describing its contents.

8. Documents produced in response to this request shall be produced together with copies of file labels, dividers, or identifying markers with which they were associated when the request was served.

9. When you produce documents, you should identify the paragraph(s) or request(s) in the Committee's letter to which the documents respond.

10. The fact that any other person or entity also possesses non-identical or identical copies of the same documents shall not be a basis to withhold any information.

11. The pendency of or potential for litigation shall not be a basis to withhold any information.

12. In accordance with 5 U.S.C.§ 552(d), the Freedom of Information Act (FOIA) and any statutory exemptions to FOIA shall not be a basis for withholding any information.

13. Pursuant to 5 U.S.C. § 552a(b)(9), the Privacy Act shall not be a basis for withholding information.

14. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.

15. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) every privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author, addressee, and any other recipient(s); (e) the relationship of the author and addressee to each other; and (f) the basis for the privilege(s) asserted.

16. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (by date, author, subject, and recipients), and explain the circumstances under which the document ceased to be in your possession, custody, or control.

17. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents that would be responsive as if the date or other descriptive detail were correct.

18. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data, or information not produced because it has not been located or discovered by the return date shall be produced immediately upon subsequent location or discovery.

19. All documents shall be Bates-stamped sequentially and produced sequentially.

20. Two sets of each production shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2105 of the Rayburn House Office Building.

21. Upon completion of the production, submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control that reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term "document" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, data, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, communications, electronic mail (email), contracts, cables, notations of any type of conversation, telephone call, meeting or other inter-office or intra-office communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape, or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.

2. The term "communication" means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, mail, releases, electronic

message including email (desktop or mobile device), text message, instant message, MMS or SMS message, message application, or otherwise.

3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information that might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neutral genders.

4. The term “including” shall be construed broadly to mean “including, but not limited to.”

5. The term “Company” means the named legal entity as well as any units, firms, partnerships, associations, corporations, limited liability companies, trusts, subsidiaries, affiliates, divisions, departments, branches, joint ventures, proprietorships, syndicates, or other legal, business or government entities over which the named legal entity exercises control or in which the named entity has any ownership whatsoever.

6. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual’s complete name and title; (b) the individual’s business or personal address and phone number; and (c) any and all known aliases.

7. The term “related to” or “referring or relating to,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with, or is pertinent to that subject in any manner whatsoever.

8. The term “employee” means any past or present agent, borrowed employee, casual employee, consultant, contractor, de facto employee, detailee, fellow, independent contractor, intern, joint adventurer, loaned employee, officer, part-time employee, permanent employee, provisional employee, special government employee, subcontractor, or any other type of service provider.

9. The term “individual” means all natural persons and all persons or entities acting on their behalf.