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

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

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.

Although Microsoft is not in general obligated to notify its customers of anomalous traffic and suspicious behavior that we've not yet confirmed could be malicious or that does not otherwise rise to the level of an information system security or cyber incident,[1] in the US, as a provider to federal customers, Microsoft cloud services, including Office 365, are required to meet or exceed requirements established by the Federal Risk and Authorization Management Program (FedRAMP) as well as Defense Federal Acquisition Regulations (DFARS). FedRAMP and DFARS require cloud providers to track and document incidents and to report them to agency customers, US-CERT, and other federal points of contact associated with the FedRAMP program.

Federal agencies monitor for anomalous traffic or suspicious behavior,[2] and FedRAMP-approved cloud providers may help enable agencies engage in and manage such monitoring. Microsoft offers a wide range of data protection products and features designed to enhance our customers' ability to monitor and defend their own data, networks and environments. Currently these products are available through two contract models: either as part of a suite, or as a stand-alone product. Offered suites include Microsoft 365 G3 and Microsoft 365 G5. G3 includes core solutions for security, compliance, identity, and management; the G5/E5 suite includes additional advanced solutions.[3] For the different levels of logging capabilities available by contract or license, please see the response to Question 4 below.

While we are not legally required to monitor for and notify customers of anomalous traffic or suspicious behavior that do not rise to the level of an information system security or cyber incident, we do continuously monitor and perform ongoing security assessments as part of our overall security policies, practices, and procedures. This continuous monitoring process includes reviewing telemetry and other cloud usage patterns and determining whether the set of deployed security controls in our cloud systems remain effective in light of new exploits and attacks. When we observe suspicious behavior that we associate with one of the many nation-state actors tracked by the Microsoft Threat Intelligence

---

[1] FedRAMP defines an "information system security incident" as any suspected or confirmed event that results in the potential loss of confidentiality, integrity, or availability to assets or services provided by the authorization boundary. *See* CSP_Incident_Communications_Procedures.pdf (fedramp.gov) at 6. DFARS 252.204-7012 defines a "cyber incident" as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. *See* 252.204-7000 Disclosure of Information. (osd.mil).

[2] *See, e.g.*, practices in NIST 800-53 Rev. 5, the NIST Cybersecurity Framework v1.1, and Trusted Internet Connections 3.0.

[3] For a comparison of what's included in G3 and G5 suites, *see* Microsoft 365 Government.

Center (MSTIC)[4] and that we think indicates a threat or compromise of a customer's Office 365 account, we do notify the customer of the threat and provide any actionable information.

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.

Microsoft has received requests from several government customers in the wake of recent attacks and has been providing support, including for the U.S. government. However, Microsoft cannot comment on specific customer requests due to confidentiality obligations. Any questions about government agency requests for monitoring support are best directed to U.S. federal agencies. In addition, Microsoft's Detection and Response Team (DART)[5] has been working with customers to help them better understand particular threats and risks in their operating environment, particularly following in the wake of the NOBELIUM[6] attack. We also work with customers to ensure they understand the capabilities of the security services available to them in Azure and Microsoft or Office 365; these services provide great visibility into the security of their environment and threats against them.

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.

The Chief Information Officers at each agency and department can best provide information about whether and how they utilize the various logging capabilities that they have available.

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.

[4] Microsoft uses threat intelligence to protect, detect, and respond to threats
[5] Microsoft Detection and Response Team (DART)
[6] Nobelium Resource Center – Microsoft Security Response Center

The logging capabilities for Microsoft licenses for federal customers include either Basic Audit[7] or Advanced Audit.[8]

Basic Audit captures more than 400 events from dozens of services, and audit records are stored for 90 days. Using the Application Programming Interface (API) referenced below, customers can also search audit logs, export the raw data, and format it into an Excel file, which they can then store and use as they deem appropriate.

Advanced Audit, for the Office 365 and Microsoft 365 Government environments, captures two additional events beyond those events for which there are logging reports provided by Basic Audit; these events are associated with users accessing and sending mail items.[9] With Advanced Audit, audit records can also be stored for longer than 90 days. All Exchange, SharePoint and Azure Active Directory audit records are retained for one year by default.[10] Advanced Audit also allows administrators to set policies to increase the retention period of other audit records from the default of 90 days to one year. With an additional add-on license, audit logs can also be retained for 10 years.

Both Basic Audit and Advanced Audit enable collected audit records to be accessible through the Office 365 Management Activity API. The API allows customers to export audit records for their own use and retention, with Advanced Audit providing faster performance.

The licenses that are available for federal customers and include Basic Audit are:

- Office 365 Government F3
- Office 365 Government G1
- Office 365 Government G3
- Microsoft 365 Government G3

The licenses that are available for federal customers and include Advanced Audit are:

- Office 365 Government G5
- Microsoft 365 Government G5

There are two separate optional bundles of features that can be combined with the Microsoft 365 Government G3 license to add Advanced Audit. These include:

- Microsoft 365 G5 Compliance
- Microsoft 365 G5 eDiscovery and Audit

Pricing depends on many factors, including whether a customer chooses to procure services based on an offered suite or as stand-alone products. The Microsoft 365 G5 eDiscovery and Audit add-on is the smallest increment that increases a customer's audit record retention from 90 days to one year; the add-on includes some additional features beyond Advanced Audit.

---

[7] Search the audit log in the Security & Compliance Center - Microsoft 365 Compliance | Microsoft Docs

[8] Advanced Audit in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs

[9] Advanced Audit in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs; note that, beyond Office 365 and Microsoft 365 environments, Advanced Audit provides logging reports for two additional events related to conducting searches in Exchange Online or SharePoint Online (i.e., Advanced Audit captures four additional events total for other environments).

[10] Manage audit log retention policies - Microsoft 365 Compliance | Microsoft Docs

We appreciate that some U.S. federal customers have recently raised questions about the costs associated with Advanced Audit and their ability to store audit logs with Microsoft for a longer time period. While we work to address their questions and work collaboratively toward a long-term solution, we are now offering all U.S. federal customers that use our Government Cloud a one-year free trial of Advanced Audit. More details are available in our recent announcement: Addressing Audit Log Storage for U.S. Federal Government Customers - Microsoft in Business Blogs.

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.

Microsoft takes confidentiality and security very seriously. Information about an individual customer's security posture and any security incident is sensitive, non-public information that Microsoft protects in accordance with the non-disclosure and confidentiality obligations in its license agreements. These terms and conditions prohibit Microsoft from disclosing the details of a breach to a third party unless required by law or directed by the customer. While the "U.S. Government" may be a distinct entity, products and services are procured by agency; thus, the agency is the contracting party.

Standard confidentiality language from our license agreements include:

> *"Confidential Information" is non-public information that is designated "confidential" or that a reasonable person should understand is confidential, including Customer Data and any Statement of Services. Confidential Information does not include information that (1) becomes publicly available without a breach of this agreement, (2) the receiving party received lawfully from another source without a confidentiality obligation, (3) is independently developed, or (4) is a comment or suggestion volunteered about the other party's business, products or services*.

A notification of a cyberattack, or a request for assistance or support, would qualify as confidential information, a conclusion shared by federal agencies that are Microsoft customers.

Our agreements also state:

> *Neither party will disclose that Confidential Information to third parties, except to its employees, Affiliates, contractors, advisors and consultants ("Representatives") and then only on a need-to-know basis under nondisclosure obligations at least as protective as this agreement*.

This language ensures that confidential information is protected by both parties to the agreement. In this case, that includes any entity that is not a party to the contract or covered by the defined term "Representatives," including other agencies of the U.S. government or even other branches of the U.S. government, a conclusion shared by federal agencies that are Microsoft customers.

Another standard contracting term, which is also present in Microsoft's agreements, includes:

> *A party may disclose the other's Confidential Information if required by law; but only after it notifies the other party (if legally permissible) to enable the other party to seek a protective order*.

In the case of the NOBELIUM attacks against U.S. government agencies, a law requiring notification to another agency would have enabled Microsoft to notify customers of our obligation to disclose and our intent to comply with that legal obligation. At present, we need to request customer (the victim) permission to disclose that customer's confidential information (the attack) to a third party (i.e., the Dept. of Homeland Security). A legislative solution or executive action could address that issue and enable notification of incidents that meet whatever criteria are set in law.

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

Microsoft does not have a breakdown of costs associated with the NOBELIUM response. Our internal incident response teams were mobilized as a part of our response, and Microsoft provided support to our customers, partners, and governments needing engagement during the incident.

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?

Due to our size and the nature of our risks, conventional errors and omissions insurance is not available to Microsoft. In lieu of such coverage, we self-insure extensively and supplement with a 'manuscript' insurance program that is tailored to Microsoft's needs and that covers a slice of the spectrum of risks that would typically fall into the errors and omissions line of insurance coverage. This program also includes a very large self-insured retention that Microsoft would bear before the insurance would begin to apply. With regard to this matter, we expect any impact to be self-insured.

We have not submitted any *claim* regarding the SolarWinds event. We have submitted a "notice of circumstance which may give rise to a claim." This notice has the effect of designating to the 2020 policy period any future claim which may arise from this event, although we have not made any determination to raise such a claim given that we expect any impact to be self-insured.

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

Since no claims have been submitted, no recovery is anticipated.

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

The insurance industry is currently experiencing a "hard market" for cyber insurance, meaning that, as insured losses have grown in recent years, insurance premium rates are increasing, and underwriting is growing more restrictive. Though we have not filed claims, we have experienced premium rate increases and anticipate future increases roughly in line with general trends.

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?

With respect to this risk, we are not currently using any "internal mechanism," such as captive insurance, to manage the exposure.

Twenty-eight insurance companies have positions in the manuscript insurance mentioned above. While we do not have express permission to disclose their names publicly, we engage with nearly every acceptably rated (i.e., financially stable) insurance company that is willing to offer acceptable terms, pricing and capacity.

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

Microsoft does not maintain such a list. The National Association of Insurance Commissioners (NAIC) has published their 2019 Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement, which shows the top twenty *standalone* and *package* cyber insurance companies by direct premium written and market share, using 2018 data.

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

Microsoft does not directly know, collect or publish data on the extent of cyber insurance coverage across our industry or across our competitors. Trade press, insurance enterprises and industry associations do report such data. To disclose that a particular company has cyber insurance has become a risk in itself, as attackers are now known to target ransomware against companies that are insured.