

**Questions for Kevin Mandia, Chief Executive Officer, FireEye, Inc.
February 26, 2021, Hearing: “Weathering the Storm: The Role of Private Tech in the
SolarWinds Breach and Ongoing Campaign”**

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

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

FireEye did not participate in nor do we endorse this report, but a [2020 study](#) conducted by IBM and the Ponemon Institute found that the average cost of a data breach is \$3.8 million or \$150 per lost record.

Questions from Representative Jim Cooper

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?

We have submitted first-party claims for expenses related to a privacy event and a crisis event (the same event). There are no third-party claims at this time. The expenses we are seeking reimbursement for are attorneys as breach counsel and support for privacy/crisis event issues; a public relations firm’ computer forensic services, including Mandiant, Microsoft, and KLDDiscovery.

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

The total amount to be paid by our insurers is to be determined, as the claim is still in process and we do not have a reasonable estimate of total reimbursements at this time.

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

Yes, premiums will increase, though it is difficult to estimate by how much premiums depend upon various factors (i.e., the claim, market conditions).

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?

We carry several layers of E&O/cyber insurance, though the names and our contracts with those carriers are confidential for both us and the carriers.

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

It is our understanding that most major insurance companies provide this coverage to organizations in our industry, including for example, AIG, Beasley, CNA, Chubb, AXA XL, Travelers, Zurich, AXIS, HCC, and Hartford, etc. Various factors are considered for selecting an E&O/cyber insurance provider (e.g., industry, size, sophistication, etc.). Customized factors are considered as well, such as the carrier’s claims paying processes and negotiations related to coverage language.

**Questions for Kevin Mandia, Chief Executive Officer, FireEye, Inc.
February 26, 2021, Hearing: “Weathering the Storm: The Role of Private Tech in the
SolarWinds Breach and Ongoing Campaign”**

Some of these factors include ensuring an insurance program is customized for the client, partnered with providers that have good claims paying processes, negotiating coverage language, etc.

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

According to one insurance carrier, coverage varies from company to company. In related tech industries, the purchase rate is about 90% for tech E&O/professional liability and about 60% for cyber. This is about 2-3 times higher than the purchase rate for all industries. It is our understanding nearly every firm in our industry has this coverage. To the best of our knowledge, all of our main competitors carry this coverage. We expect the purchase rate for cyber coverage to increase based on the increasing number of cyber incidents.