**Slide 1**

Dear Board of Directors, executive team, and other stakeholders: Thank you for taking the time out of your busy day to meet with me as I, at a high level go over BlackRock’s proposed strategic cybersecurity plan, which I and my team have been working on over the past few months. So, let’s get right into it.

**Slide 2**

First, you might be wondering what exactly this plan is. Well, it is a two-part document drafted with the aim of keeping the organization secure and prepared for any incidents that may arise in the realm of information security.

**Slide 3**

So, why do we exactly need such a plan on top of our various security policies and procedures? Well, there are many reasons why.

* First, we rely on advanced IT systems to meet daily business operations as well as power asset management services and products to create exceptional financial future for customers, all aligned with our Business Mission and Vision.
* The other reason is our commitment.
  + As a global leader in investment, asset management, and risk management advisory, we are expected to deliver exceptional investment platforms and services.
  + We also need to understand our clients’ concerns in regards to protecting their personal information that we collect and share to run our daily functions, depending on our products or services that they utilize.
* However, we face potential threats from fluctuating investment and world economy, as well as changing rules and reforms.
* We also face security risks arising from technologies, third-party interactions, and security breaches.
  + This includes cyber-attacks on our telecommunication systems as well as phishing and ransomware.
  + Plus, security upgrades on systems can disrupt the investment and trading platforms that our customers use.
  + Moreover, as we have seen before, there can be unavailability or failure of technical dependencies from third parties.
* All of these can lead to severe fines for violating compliance standards and privacy policies.

Hence, we need to be cognizant about all these issues and address them appropriately through technical and administrative controls.

**Slide 4**

So, how do we go about executing such a plan? The answer is: A collaborate effort is needed. That is, beginning with the information security department playing a critical central role in ensuring the company’s products and services are available for business operations and continuity, to employee buy-in and your support as executives and leaders are all essential.

Hence, going back to the security department, in alignment with its core values, the team

* Identifies, assess, and proactively manages the risks to BlackRock's information systems and data.
* As well as works to establish high availability of the technologies needed for business, given the time-sensitive nature of investment management.

**Slide 5**

The security team also supports security metrics reporting so that we can use to analyze performance and make appropriate risk mitigation or acceptance decisions. For example,

* + **Time to Access Resources:** This measures the loss in productivity when users are unable to access their accounts, which can cause some degree of financial loss for BlackRock.
  + **Time to Remediate Incidents:** This measuresthe time it takes to remediate security incidents related to company assets, indicating the value of our information security program delivers.
  + **Next, Security Awareness Rate:** This measures the completion rate of staff security awareness training and campaigns, which can be used for internal compliance and auditing purposes.
  + **Lastly, Patch Management Coverage:** This measures the patch policy compliance of servers to identify our risk posture as well as track vulnerabilities.

**Slide 6**

As I mentioned before, we heavily rely on IT systems for business activities. However, in the information security space, we believe that anything that can go wrong will go wrong. Hence, we incorporated a maintained Business Continuity Plan (BCP) in our proposed strategy. The information for analysis is derived from the Business Impact Analysis (BIA) that we have done on the company’s highly-valued assets that are critical for daily business operations.

Through the Business Continuity Plan, we can ensure that critical business operations can continue when unplanned events or emergencies occur. To achieve this, we make use of our backup hot site, which houses all the necessary equipment and data needed for us to go live in minutes. Again, this is very important due to the time sensitive nature of our industry.

**Slide 7**

In alignment with BCP, as a sample, we also incorporated a Disaster Recovery Plan for our high revenue generating and expensive asset, Aladdin OS, which hosts our investment platform that clients use on daily basis.

In the event that the entire system has to go back to full functionality after a crisis, the procedures include actions from notifying the right individuals, to investigating, testing, and migrating data from the hot site back to the primary site.

**Slide 8**

That said, for the plan to have its long-lasting goals and rewarding results, some essential elements are needed. The first one is regular revision and maintenance of the plan as appropriate.

The second and probably the more important one is continual support and funding to address the discussed key areas including Hardware, software, and to establish a security-aware well-rounded workforce. The other major part of the funding is need to attract, train, and maintain employees for the large size of the security department, which as shown here contains more than 500 associates around the globe.

**Slide 9**

So that completes the detailed content about the strategic plan. However, I have also prepared some excellent industry sources, which I promise are not technical, if you wish to check them out when I send out this presentation. I think you might find them interesting to see where our strategic cybersecurity plan can take us.

**Slide 10**

Now, I want to use the remaining few minutes to answer any questions or gather any feedbacks and comments. Again, we will be discussing about this plan more in our upcoming weekly leadership meeting. Thank you for your time!