STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

Office of the President

Tel 201 216 5213

Fax 201 216 8250

September 9, 2019

To the Stevens Community:

As the semester is now well underway and we have welcomed new cohorts of undergraduate and graduate students to Stevens, I want to extend my warm greetings to all our faculty, staff, and—especially—our students. I hope you all join me in making the 2019-20 academic year one that is memorable for all that we will accomplish together.

In the early weeks of the fall semester, I typically send a message to the Stevens community with an update about our new students and highlights from across the university; you will receive that memo soon. Today, however, I write to you about the August 8th cyber-attack that disrupted the entire Stevens community as we closed out our summer programs and prepared for the fall semester.

There have been many questions about the nature of the attack; its impact on our systems, operations, and data; and the measures we are taking to further harden Stevens' networks and systems against future attacks. Now that our critical and essential systems are more secure and stable and much of the campus has returned to normal operations, I would like to provide a more detailed account of the incident, how we responded, and how we plan to further strengthen the security of Stevens' networks.

The Cyber Attack:

On August 8, 2019, approximately 75 members of our community encountered a ransom message upon logging in to the Stevens network. The message did not specify a ransom amount. Based on our forensic investigation, we now know that the ransom message was prompted by a sophisticated malware attack on the Stevens network, which subsequently encrypted a number of on-campus systems and the data they contained. It is the case that these types of attacks typically begin with phishing emails; however, our investigation has not definitively determined that this was the origin of the Stevens cyber-attack.

Our Response:

The Division of Information Technology (IT), supported by our cyber security partner, took immediate action to contain the attack and to preserve and protect Stevens' network, systems, and data. IT immediately implemented the Cyber Incident Response Protocol (CIRP), a plan based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework established and recommended by the Department of Homeland Security for government and public organizations.

IT quickly disabled the network and all accounts in order to accelerate our ability to restore and, in some cases, rebuild a more secure and stable environment. The network outage, therefore, was not caused by the malicious efforts of those who launched the cyber-attack, but was rather a precautionary measure to contain the attack.

The Emergency Management Team (EMT) was convened on the afternoon of August 8th to assess the impact of the cyber-attack and triage the problems it caused. The EMT is a committee comprising administrative and academic leadership representing key units and constituencies throughout the university. This group continued to meet once or twice daily, seven days per week until August 30th, and it continues to meet regularly as of this writing. Through the EMT, priorities were established and resources were allocated in order to support critical operations with the primary goals of: (1) starting the fall semester on time on August 26th; and (2) completing the summer courses that were underway at the time of the attack. In order to accomplish these paramount objectives, dozens of tasks needed to be completed—from restoring user accounts to testing individual computers and hardware, from enhancing network security to restoring the interfaces between more than a hundred systems used by various units within the university, and many, many more.

Through these efforts, critical systems were returned to operation securely, in most cases within days of the attack. Remaining systems and functions, including discipline-specific teaching and research labs have either been restored or are expected to be back online in the coming days. Most systems are now operational, including at least 46 that have already been placed back into operation. Efforts are continuing to prioritize and address remaining issues, e.g., networked printing, desktop computers, etc., as we strive to ensure that all users are able to perform their responsibilities in a secure network environment.

Response to Ransom Demand and Findings to Date:

Importantly, the ransom demand was unsuccessful. Stevens did not make a ransom payment in any capacity, as our assessment was that damage to critical onsite systems would be minimal and could be effectively mitigated. Significantly, many IT systems had been migrated to the cloud in the aftermath of 2012's Superstorm Sandy, a measure Stevens undertook to strengthen its business continuity efforts. This measure proved to be essential to our recovery efforts, as did the robust data backup systems that were in place that enabled the restoration of critical data when necessary.

With the help of our cybersecurity partner, a forensics investigation began soon after the incident. Findings to date suggest that the objective of the attack was to extract a ransom payment by encrypting data and disrupting operations. This type of attack has different characteristics than those intended to exfiltrate personal data. While the forensic investigation is ongoing, to date there has been no evidence that any data, including personal or financial data, has been exfiltrated or viewed by any unauthorized individual as a result of this incident.

One question I often hear is, “Who was responsible for this attack?” At this time, the identity of the attacker is not known, and unfortunately, in many cyber-attacks of this nature—which have become alarmingly frequent—the perpetrator is not definitively identified.

Next Steps:

Looking ahead, we intend to learn from this experience and take additional steps to help protect our community against similar attacks. This will include further hardening our systems; developing policies that help us improve the security of our network and systems environment as a whole; and offering additional training and educational resources to all members of our community. While mitigating the risk to the Stevens community of future cyber-attacks, we are equally committed to protecting the freedom of academic inquiry and exploration. Information sharing remains central to our mission as a research university. We are committed to ensuring that our next steps equally balance reinforcing the security of Stevens’ systems and networks with enabling and promoting the open discovery of knowledge.

In closing, I want to extend my sincere appreciation to all members of the Stevens community for their patience and understanding throughout the past several weeks. It would be an understatement to say that this cyber-attack caused significant disruption to our community. However, this episode has also been a vivid illustration of one of our strategic priorities, *Through Collaboration, Impact*. The focused, systematic, and determined approach exhibited by so many colleagues throughout the university to solve problems—one after another—with the goal of starting the semester on time was nothing short of awe-inspiring. As the important work to fully restore and protect our network continues, I am immensely grateful for the commitment and dedication—and the sheer stamina—of all my colleagues who are working to ensure that our faculty and students can pursue their academic endeavors in a secure and stable network environment.

Per aspera ad astra,

Nariman Farvardin
President