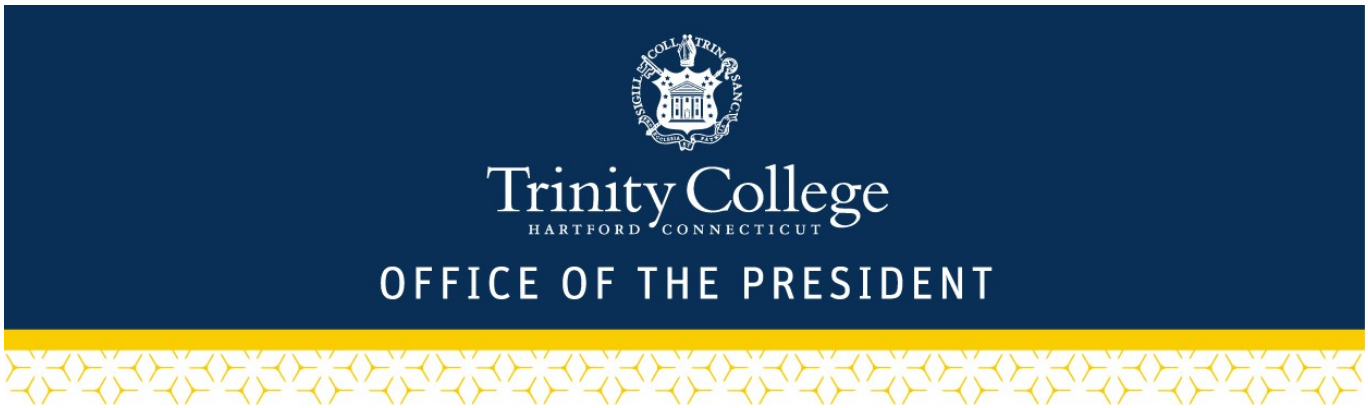
# Update on Cybersecurity Incident

President Joanne Berger-Sweeney <President@trincoll.edu>
Tue 11/24/2020 2:34 PM
**To:** President Joanne Berger-Sweeney <President@trincoll.edu>




November 24, 2020

Dear Trinity College Community Members,

As many of you will recall, the college was the target of a sophisticated cyberattack that disrupted our network systems for several days in September. One of the immediate action steps we took was to launch a thorough investigation into the attack, to discern exactly how it happened and to assess its full scope and impact. That investigation, conducted by CrowdStrike—one of the world's top cybersecurity firms—is now complete, and I write today to share its findings with the broad Trinity community.

It's an unfortunate reality that Trinity is among thousands of institutions that have been hit by cyberattacks, and we know that educational institutions, many of them relying more than ever on web-based technology to teach and learn and to manage operations amid the pandemic, have been hit especially hard this year. The rapid response of our Information Services team kept this situation from being much worse, and consultation with the Audit and Risk Committee of Trinity's Board of Trustees, many of whom have professional expertise and experience in this realm, was invaluable. Additionally, I'm grateful for the support of Matthew Prince '96, CEO and co-founder of Cloudflare, whose counsel we sought early on and who was instrumental in securing the services of CrowdStrike.

Fast action on the part of the Trinity team meant the attackers had limited access to and time on our servers and therefore did not succeed in their objective of encrypting the environment and then promptly demanding ransom. To date, we have not received any such demand. The investigation did, however, reveal that two datasets from Trinity servers were accessed. One contained historical data (from 2013 and earlier) on donations by individuals and institutions. The information accessed was largely what Trinity and many other schools typically have reported publicly in annual donor rolls. **No social security or driver's license numbers were accessed, nor was any personal financial, banking, or health information**. While none of the advancement data affected is of the type that legally requires notification, we felt it important to share this information with all of you.

The other dataset contained admissions data and a limited amount of biographical and demographic information, including full name and date of birth. In two U.S. states—Washington and North Dakota—that combination of full name and date of birth is considered Personally Identifiable Information (PII),

requiring notification by the college, and we are in the process of communicating to those affected individuals.

For those who were part of the most recent admission cycle (2019-20), the data breach also involved some application file data, including admissions decisions. We are reaching out to those individuals directly as well. **Again, no social security or driver's license numbers were accessed, nor was any personal financial, banking, or health information**. This data isn't of the kind that would require notification, either, but here, too, we wanted to go beyond what's legally required in informing our community.

Please accept my sincere apologies on behalf of the institution for any concern this incident may cause. Please also know that in addition to conducting a comprehensive investigation, we have taken numerous steps to enhance security and help prevent future attacks. We have purchased and installed on all of our servers and critical workstations advanced anomaly detecting software, which is monitored 24 hours a day by cybersecurity professionals. We have increased the blocking and sensitivity of our firewall detections. We have rebuilt much of our authentication systems and required all users to change their passwords, and we are accelerating the implementation of multifactor authentication (that is, requiring more than one verification of identity to access Trinity systems).

Cyberattacks are increasingly common and sophisticated. Everyone, whether they were affected by this incident or not, should remain vigilant toward any suspicious activity, regularly update passwords, and consider other precautionary measures to protect personal information. Trinity is committed to maintaining the privacy of personal information with which we have been entrusted. We will continually evaluate our practices and internal controls to enhance security. Should you have questions related to this incident, please reach out to cyberincidentinfo@trincoll.edu.

Sincerely,

Joanne Berger-Sweeney
President and Trinity College Professor of Neuroscience