



Advances in Cybersecurity

A little over a week ago, I had the opportunity to participate in a discussion panel for Cybersecurity Awareness Month hosted by Kelly Poto who leads our Cybersecurity Internship Program. Our discussion ranged in topics from 5G, to securing future devices, to ethical issues in cybersecurity. After the panel concluded, I started to reflect on where we are as a division with cybersecurity, we have done a great deal of good things over the last 12-18 months as a team. The work we have done in this time will help us accomplish even more in the future.



Growing & Involving Our Team

If we look back just two years ago, we had only a few team members focused on IT security and our budget was sorely lacking. Thanks to the hard work of a number of people, we now have a Cybersecurity team that includes Research Security, PCI (Payment Card Industry) compliance, Incident Response (newly hired!), and an upcoming recruitment for a User Awareness and Training coordinator. Additionally, we have a terrific Cybersecurity Internship Program which includes 12 students (undergraduate and graduate) involved in research and adding to our operational areas more and more every day. If you haven't already, check out the [19-20 CSU Cybersecurity Internship Annual Report](#) to learn more about what this group has accomplished this year.



We've also developed a cross-divisional "Cybersecurity Services Team" that brings together a group of operational technology experts. Led by Angie Asmus, this team is working together to look across our entire division and ensure that we are coordinating and communicating our efforts

on operational security. Currently, this team is helping us with an asset management process for hardware; one of the foundational components to an effective Cybersecurity program. As you can imagine, it's tough to protect things if you don't know where everything lives.



We also recently launched a “Cybersecurity Initiative” which is an additional group of divisional team members led by James Cizek. One of our 2020 strategic initiatives, this group is working to help address web vulnerabilities and endpoint management in Central IT.

Investing in Cybersecurity

In addition to bringing on more team members, we've also been busy getting additional funding to invest in our Cybersecurity efforts. Over the last year, we received over \$1.3 million in one-time funding from the CSU-System that we have combined with a bit of divisional funding to invest in:

- An external security review and consultation based on the NIST Cybersecurity Framework
- End-user training and awareness
- ELK logging/monitoring
- CUI (Controlled Unclassified Information)/HIPAA infrastructure
- Network firewalls

Creating a Sustaining Program

Our goal going forward is to continue to grow our Cybersecurity program here at CSU. Our Chief Information Security Officer, Steve Lovaas, has outlined a set of steps that he'll be leading in the coming year(s) that will create new directions and take a strategic approach to Cybersecurity. Some of those key items include:

- Annual NIST Cybersecurity Framework “Target Profile”
- Annual self-assessment with National Cybersecurity Review
- Further incorporating our interns into operational units
- Exploring a CSU-System wide Cybersecurity approach



Continuing to Evolve

I encourage you to look at all the things happening in Cybersecurity as a great example of where we've been able to invest in people and resources. It's tremendous to see how much we can accomplish in a short period of time if we do it together as a team. Our hope now is to take approaches like



this and apply it to other areas in our division for further evolution and growth.

Thank You

Thanks to everyone who has had a hand in evolving cybersecurity in our division. You are much appreciated and respected. Thanks for all that you do.

Take care and stay safe everyone,

-Brandon

A handwritten signature in black ink, appearing to be the name 'Brandon', written in a cursive style.