INSIDE HIGHER ED

Cybersecurity in Academic Research

An *Inside Higher Ed* webcast

Tuesday, October 4, 2022

2 p.m. Eastern

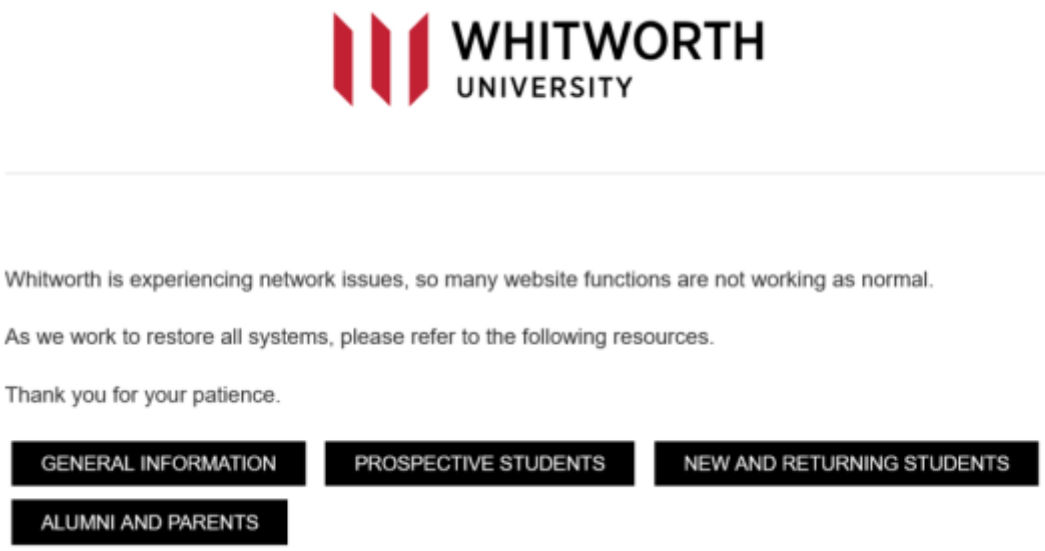
Presenter

- Scott Jaschik, editor, *Inside Higher Ed,* scott.jaschik@insidehighered.com

What (Some of) Our Headlines Say

- Ransomware Attacks Against Higher Education Increase
- Cyberattacks Against Colleges Add to Financial Strain
- Colleges Are ‘Juicy Target’ for Cyberextortion
- FBI Warns of Increased Ransomware Attacks Targeting Colleges
- And many others…

What Happened at Whitworth?



Why Higher Ed Tempts Cyber Thieves

- Apparent wealth
- Total reliance on technology
- Faculty produce research worth ???
- Some (many?) faculty resist cybersecurity

Why Faculty Resist

- Traditions of academe
- Sometimes, colleges and universities do a poor job of explaining things.

What Is Changing? Colleges Pay

- “You can collect that money in a couple of hours,” a ransomware hacker’s representative wrote in a secure 2020 chat with a University of California, San Francisco, negotiator about the $3 million ransom demanded. “You need to take us seriously. If we’ll release on our blog student records/data, I’m 100% sure you will lose more than our price what we ask.”
- The university later paid $1.14 million to gain access to the decryption key.

INSIDE HIGHER ED

What Is Changing? The Volume

- The number of attacks on colleges and universities is increasing.
- Nearly three-quarters (74 percent) of ransomware attacks on higher ed institutions succeeded. Hackers' efforts in other sectors were not as fruitful, including in business, health care and financial services, where respectively 68 percent, 61 percent and 57 percent of attacks succeeded, according to a report from Sophos.

What Is Changing? Is Higher Ed in Worse Shape Than Others?

- Among all sectors in 2021, higher education had the slowest recovery times following an attack, according Sophos. Forty percent took more than a month to recover—in contrast to the global average of 20 percent.
- The average remediation cost of $1.42 million was higher than the global average for all sectors.

What Should the U.S. Do?

Create a White House coordinator

--From Tracy Mitrano

What Should Colleges Do? Talk Openly

Millersville University 2021

MESSAGE FROM PRESIDENT WUBAH

MARCH 17, 2021

Dear Millersville University Community,

As you are aware, Millersville University has been a victim of a cyberattack. We have engaged law enforcement and global security experts and we are continuing a thorough forensic investigation. We have now been informed by our cybersecurity experts that it appears personal information from a handful of individuals has been disclosed. Those few individuals who were impacted will be notified and provided resources according to Pennsylvania state law.

On behalf of my leadership team, we regret that this attack happened and the inconvenience it has caused our community members.

It is important to recognize that we are the victim of a crime. Millersville receives 9 million cyber intrusion attempts daily. We use many layers of security to protect our networks and systems including anti-virus, firewalls and application scanning, as well as proactively monitoring for vulnerabilities and suspicious activity. However, no system is 100 percent secure.

The University will continue to work with law enforcement and cybersecurity consultants to determine who is responsible.

Millersville University holds cybersecurity as an institutional priority. Over the past two years, we embarked on a strategic technology plan to enhance the network's security, systems and data. IT had begun implementing Multi-Factor Authentication and many of the University's mission-critical resources were migrated to the cloud. The timing of this attack was unfortunate because not all of the planned initiatives had been completed. The initiatives that begun are being incorporated into the network restoration process and other enhanced security protocols that meet or exceed industry standards and best practices.

As a reminder, the following resources are available (https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure) to strengthen your knowledge to safeguard your digital presence.

I share your concerns and recognize the frustration of our community. Our institutional and, in some cases, individual privacy has been violated and our systems and services have

What Can Colleges Do Beyond Talk?

- Colleges can use encryption.
- They can secure access to such items as payroll and student records.
- Faculty research?

Dealing With Threats From China

Solutions offered by Ted Mitchell, president of the American Council on Education:

--Establish a working group of key officials to review policies and compliance with regulations.

--Develop a relationship with local FBI field office.

--Educate and train all faculty members.

--Ensure campus security staff and IT staff have the tools they need.

--Examine carefully any international partnerships.

Q&A

- Your questions
- Your suggestions for future coverage

With Thanks to…