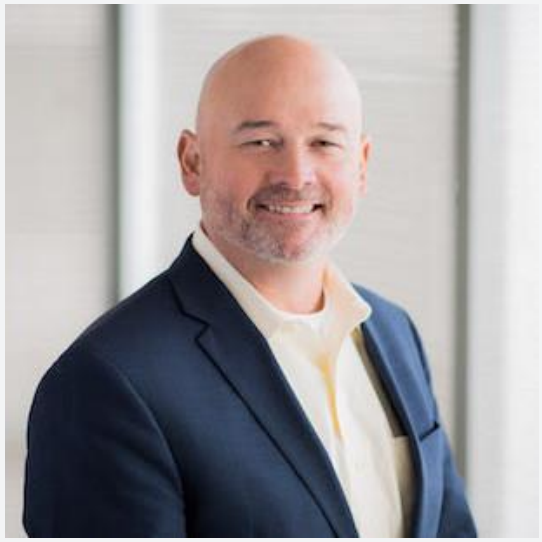
MANDIANT

Building Resiliency into Higher Ed Cybersecurity Programs

University Business Webinar – October 11, 2022

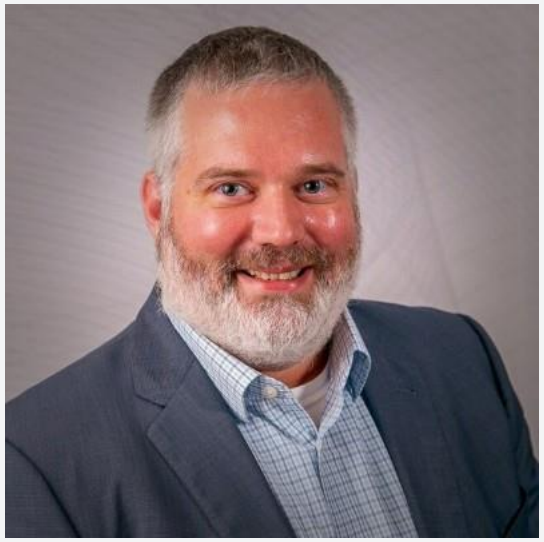
Introducing our panelists ....

Monte Ratzlaff



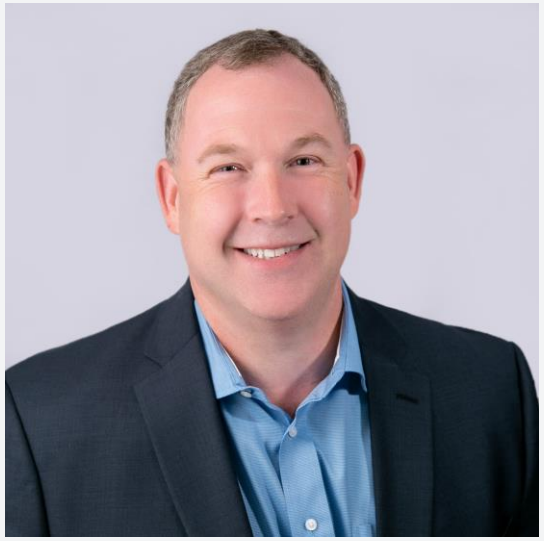
University of California Office of the President
Director, Cyber Risk Program

Chris Schreiber



Campus CISO
Owner / Higher Education Cybersecurity Strategist

Jon Ford



Mandiant
Managing Director, Global Government Services & Insider Threat Risk Solutions

Discussion Question 1

What are some of the top challenges & priorities facing higher ed cyber security teams today?

Discussion Question 2

What can you share about threat actors targeting higher ed institutions, in terms of TTPs (tactics, techniques & procedures)?

Polling question 1:

Which cyber threats pose the biggest challenge for your higher ed organization? (Please choose all that apply.)

- Research and Data compliance
- Email based attacks (Ransomware, phishing, etc.)
- Supply chain security (vendor partner security)
- Lack of cyber awareness amongst students, faculty and staff
- Insider threats

Discussion Question 3

We know that Securing data across higher ed organizations-- from student/faculty/staff data, to research data, to healthcare data -- is a top priority to get ahead of threat actors. What are some strategies that work and enable these organizations to take a more proactive stance?

Discussion Question 4

According to Mandiant's M-Trends 2022 Report, 25.8% of investigated initial access came through the exploitation of public-facing applications, underscoring the importance of maintaining an up-to-date inventory of assets and vulnerabilities. To effectively mitigate risk and protect against initial compromise, higher ed organizations need to identify, enumerate and harden internet-facing devices, hosts, applications and network services.

Polling question 2:

What stage is your institution in using 3rd party solutions that are used to process and/or store sensitive data (e.g. cloud-based ERP and student information systems, research computing, etc.)?

- Already adopted
- In process of adopting
- Planning to adopt in next 12-18 months
- No plans to adopt

Discussion Question 5

Where do you recommend prioritizing immediate efforts with insight into the high-risk assets being targeted by threat actors?

Discussion Question 6

What are best practice recommendations for performing asset discovery & vulnerability detection?

What are the benefits of increased visibility?

Discussion Question 7

How is your Higher Ed organization …

- Addressing vendor risk?

- Approaching overarching security policy governance?

Polling question 3:

How do you feel about the following statement? I am confident in my organization's readiness to secure the supply chain/3rd party vendors.

- Strongly Agree
- Agree
- Somewhat Agree
- Disagree
- Don't Know

Discussion Question 8

Many organizations are considering or moving toward a Zero Trust Security model.

How will Zero Trust adoption impact higher ed institutions?

Discussion Question 9

Higher ed organizations , like those in the enterprise space, struggle with talent and technology gaps. Getting the people part of the equation is especially hard… What are some of the approaches your organization is taking to address this?

Discussion Question 10

Are there any additional core concepts that higher ed leaders and officials should be thinking about, and recommended measures that should be in place? What are some of the characteristics you'd expect to see in a more comprehensive, holistic cyber program?

Discussion Question 11

What advice can you provide on building a convincing and effective business case to help obtain buy in for security initiatives?

MANDIANT®

Thank You