Canon
CANON SOLUTIONS AMERICA

SMART CHANGE STARTS HERE.

# UNDER LOCK & KEY

## Strategies for higher ed security

"When everything is connected, everyone is vulnerable." The New York Times and Wall Street Journal best-selling author Marc Goodman provided an intensely riveting glimpse into the dark side of technological innovation and the unintended consequences of our connected world in his book "Future Crimes." For example, The Ponemon Institute's "2018 Study on Global Megatrends in Cybersecurity" shows that 67 percent of 1,100 senior information technology practitioners surveyed around the world believe they're at risk of cyber extortion.

These are the types of concerns that keep Carlos A. Fernandes up at night. As the managing principal and CEO of Agile Cybersecurity Solutions (ACS), Fernandes sits on the front lines of the cybersecurity crisis, which continues to grow in complexity and volume. The Washington, D.C.-based firm's client base is a who's who of governmental agencies and major private sector companies. Over the past seven-plus years, Fernandes has assembled a team of "Cyber SEALs" dedicated to establishing security protocols, mitigating risks, and providing incidence response when needed.

"As we ubiquitously integrate technology into every area of our lives, cybersecurity is the glue that keeps it all together," Fernandes says. "Security is a journey, not a destination. There is no such thing as 100 percent cybersecurity."

When it comes to protecting your university's digital assets, that last statement should be taken very seriously. As Fernandes freely admits, today's universities are not taking the proper precautions to protect themselves and their students from the advanced and persistent threats of cyberattacks. Most schools default to availability and ease of use versus the implementation and regular assessment of cybersecurity best practices.

In the current landscape, being proactive is the new normal. Fernandes believes that because universities are in the education business, they should lead by example when it comes to cybersecurity practices. That not only means creating risk management and threat mitigation systems, but also serving as an education resource for their faculty and students.

"People are your weakest link or your strongest defense. Everyone—your administrators, teachers, students—plays a role in protecting your organization."

*— Mark Sinanian,*
*Sr. Director Solutions Marketing, Canon Solutions America*

> "As we ubiquitously integrate technology into every area of our lives, cybersecurity is the glue that keeps it all together. Security is a journey, not a destination."
>
> *— Carlos A. Fernandes,*
> *Managing Principal & CEO, Agile Cybersecurity Solutions*

"Because of the persistent threats we face every day, you must build an effective security framework," Fernandes says. "You can no longer depend on the traditional ways of protecting yourself. It is naive to think that you can connect another 'shiny' cybersecurity product to your network and expect it to be cyber secure."

## PREDICT. PREVENT. PERSIST.

Employing what Fernandes calls an agile mindset (the framework to predict, prevent, and persist) is the key to staying ahead of the cybersecurity game and not reacting after something happens.

Asking "how" to get started the right way is the best jumping off point. "I get asked this question every day," Fernandes says. "What most people want is a checklist—a quick fix. Cybersecurity does not work like that. There is no one-size-fits-all approach."

His first recommendation is to confirm your current security posture—your "as-is." The most cost-effective approach is to hire a well-qualified cybersecurity service provider to perform a vulnerability assessment. Once you have a clear understanding of your vulnerabilities and/or gaps in your security posture, you can develop a prioritized plan for next step actions.

"Most do not need another 'shiny' product peddled from a cybersecurity vendor," Fernandes says. "In reality, what you need most is a cybersecurity professional who can assist with maximizing your existing investment."

Colleges and universities that believe they have what they need are often short-sighted. In most cases, adding another layer of protection is the best course of action. It's called avoiding the "pay me now or pay me a lot more later" mistake, says Mark Sinanian, senior director, solutions marketing for Canon Solutions America's Enterprise Services & Solutions division.

"When it comes to cybersecurity, it takes a meeting of the minds to get everyone on board, all of the stakeholders in the organization," Sinanian says.

Sinanian believes universities must take a serious look at all of the places of entry, including students in the lounge using their computers or smart devices. "Hackers are able to find any way that they can to get an in. The best way to look at it is that people are your weakest link or your strongest defense. Everyone—your administrators, your teachers, your students—plays a role in protecting the organization. Your cybersecurity is reliant on your habits."

It is estimated that over the next decade, cyber espionage against U.S. corporations from foreign actors could result in serious consequences to the U.S. economy. Fernandes recommends that U.S. corporations, including higher ed institutions, must focus on best practices, starting with the basics.

"Assess your current security posture and maximize your existing investment before buying the next great cybersecurity product," he says. "Resist the desire to complicate matters. Simplicity is key and cybersecurity's best friend."

Canon

CANON SOLUTIONS AMERICA

1-800-815-4000 CSA.CANON.COM



11/20-1061-5174