4-10-2017

RWU Cybersecurity Expert Works on State Initiative to Combat Cyber Threats

Juan Siliezar
Roger Williams University

Follow this and additional works at: https://docs.rwu.edu/weekatroger_featured_news

Part of the Higher Education Commons

Recommended Citation
https://docs.rwu.edu/weekatroger_featured_news/305

This News Article is brought to you for free and open access by the The Week at Roger at DOCS@RWU. It has been accepted for inclusion in Featured News Story by an authorized administrator of DOCS@RWU. For more information, please contact mwu@rwu.edu.
RWU Cybersecurity Expert Works on State Initiative to Combat Cyber Threats

As a founding member of the state’s Joint Cyber Task Force, RWU Cybersecurity Program Director Douglas White battles cyber disruptions in R.I.

April 10, 2017  |  Juan Siliezar

BRISTOL, R.I. – While government agencies have expanded their cyber-defense capabilities in recent years, one fact remains: because of the world’s ever-growing reliance on technology, a large-scale cyber-attack in the near future is an almost certainty. For proof, you only have to look at recent headlines and events, such as the 2016 election hacking, the Yahoo data breaches and the Sony Pictures hacking.

“Something is going to happen,” said Rhode Island State Police Capt. John Alfred, who heads the cyber crimes unit and the state’s Fusion Center. When it does, the state needs to be able to “respond to and mitigate the threat,” he said.

That’s where the Rhode Island Joint Cyber Task Force (RIJCTF) comes into place. The RIJCTF, formed in 2009, monitors and protects the state’s cyber infrastructure from natural disasters, widespread viruses and cyber-attacks. It brings together members of the Rhode Island State Police Computer Crimes Unit, the Rhode Island Emergency Management Agency, the Rhode Island National Guard
and over 150 individuals representing hospitals, finance, utilities, defense and higher education—
including RWU’s Cybersecurity and Networking Program Director Douglas White, who has been
there since the start of the initiative.

White, a recognized expert in the technology industry and one of the earliest pioneers of
cybersecurity, is a founding member of the RIJCTF and wrote much of the operating procedure and
cyber-attack training simulators the task force uses today. Through White, RWU has been an integral
part of the RIJCTF’s efforts. For example, RWU cybersecurity students have accompanied White on a
number of trainings, including one where they defended against a cyber-attack in front of U.S.
military generals, the head of the state police, and other government officials. During another
exercise, RWU students learned to think like cyber criminals when, along with White, they played
the role of cyber terrorists trying to detect if the FBI had penetrated their systems.

Known early on as the Cyber Disruption Team, the RIJCTF helped make Rhode Island an early leader
in cybersecurity. The RIJCTF was the first in the nation to bring together civilian tech experts, like
White, with local and state government to defend cyber infrastructure. At the time, White said there
wasn’t a big focus on emergency response in cyber in the government as there was in the private
sector. It was time for the government to catch up, he said.

Today, almost all states have similar cyber teams and greater capabilities when it comes to
cybersecurity. One of the ways this happened in Rhode Island was because of bridge the RIJCTF
built between the state’s agencies and its private tech sector, which created a level of trust that had
never existed before.

“If I don’t know the answer to [a cyber issue], I know I can reach out to a Doug White or a National
Grid,” Capt. Alfred said.

To Capt. Alfred’s point, the task force has been consulted on a number of investigations thus far.
White, for example, was on-site last year at a location to help solve what it had perceived to be a
cyber-threat to its data systems. Also, last year, the task force helped investigate a string of ATM
thefts in the state and, a few years back, it helped foil a cyber-attack that threatened to compromise
years of arrest records at one of the state’s police departments, Capt. Alfred said.

Along with White, members of the task force include representatives of companies such as National
Grid, Raytheon, Dell SecureWorks, RBS Citizens, CVS, Lifespan and more. Members meet quarterly
and some – like White, who is a core member – routinely take part in cyber training exercises,
including national-level exercises.

It’s important that the RIJCTF stands ready because, as made evident by recent headlines ranging
from hackings to national surveillance and the popularization of shows like USA Network’s “Mr.
Robot,” almost everyone understands what Professor White has known all along: cybersecurity is a
massive issue.

“The threat to cyber systems has been perceived by average people,” White said. Phones, personal
computers, bank accounts, data systems – “All these things are vulnerable.” People might not
understand how hacking happens, but “everyone understands the consequences.”