PDP Communiqué

A Newsletter from the
Professional Development Program, Rockefeller College

UNIVERSITY AT ALBANY
State University of New York

Effecting Cybersecurity: Integrating our Educational Defense is Key

Eugene J. Monaco, Executive Director and Public Service Professor
Professional Development Program

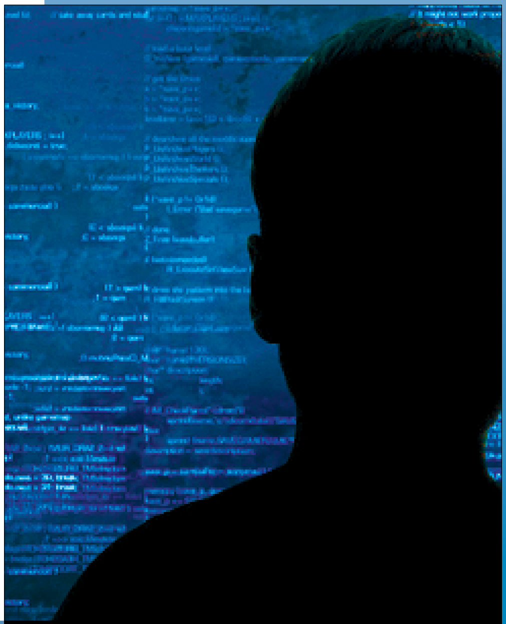
Cybersecurity is at the top of the priority lists of today's highly networked global organizations—government, corporate, education and not-for-profit alike. While ease of access to infrastructure, information and data has become the "new normal" for conducting business, our increasing transparency generates unintended opportunities for those who gain access to our data for criminal and malicious purposes. As a result, our organizations have been put on the defensive.

Recent recurring incidents of sensitive information breaches at high-profile companies, including Target, Home Depot, Staples and Sony Play, as well in government agencies as far up as the Federal Office of Personnel Management, have pushed cybersecurity concerns to the forefront of our national consciousness. The Global Risk Report of 2015, issued by the World Economic Forum, alarmingly stated that, "Ninety percent of companies worldwide recognize they are insufficiently prepared to protect themselves from cyber attacks." Our vulnerability is clear and increasing as the prevalence and scope of cyber attacks by perpetrators become even more sophisticated.

Cyber attacks result in great financial loss for the affected organizations and create significant public relations problems. Successful breaches engender enormous loss of trust not only for the specific organization affected but for the related industries, which are thereafter perceived as vulnerable. Consequently, affected organizations have been pressed to draft new policies, procedures, and regulations to defend against potential future attacks.

Our institutions of higher education are at risk as well. In 2015 both Penn State University and the University of Virginia were victims of a cyber attack; China was suspected of stealing their confidential student information. At the University of Connecticut and Johns Hopkins University, student credit card information was breached. No organization seems immune to cyber attack, and the increased frequency of attacks has raised fear that "hack attacks" and other security failures may generate widespread mayhem and greatly endanger global stability and actions

Continued on page 5



"A key piece of that solution is the alignment of our education and training programs with the knowledge and best practices of experts in the field of cybersecurity." —Eugene Monaco

VOLUME 36, SPRING 2016

Educating and Arming the Next Generation of Cyberwarriors

MARK SCHMIDT

David Rousseau

David Rousseau, Interim
Dean College of Emergency Preparedness,
Homeland Security and Cybersecurity

In his January 2015 State of the State address, Governor Andrew Cuomo announced that the University at Albany would be home to SUNY's new College of Emergency Preparedness, Homeland Security and Cybersecurity, with training programs in the New York State Preparedness Training Center in Oriskany, New York. The University at Albany was chosen for its emergency management and health preparedness training initiatives, extensive educational and research programs in homeland security and cybersecurity, and its collaborations with, and proximity to, state agencies responsible for security and preparedness.

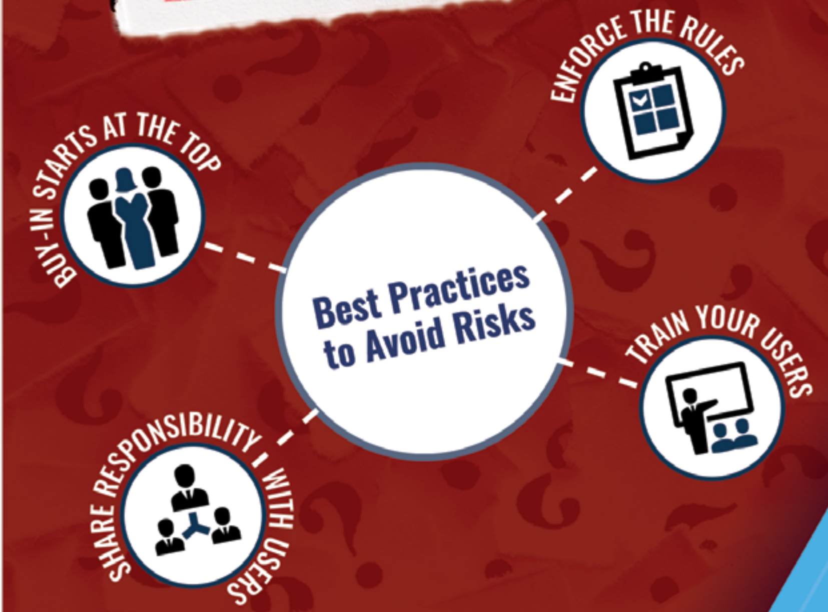
The mission of the College of Emergency Preparedness, Homeland Security and Cybersecurity is to support high-quality academic programs for undergraduate and graduate students, produce new knowledge through innovative research, and provide training and lifelong learning opportunities for professionals. These efforts will help prepare for, protect against, respond to, and recover from a growing array of natural and human-caused risks and threats in New York State and around the world.

The field of cybersecurity promises to be one of the most challenging and exciting components of the new college. Cybersecurity will be central to every aspect of human life in the 21st century. From an economic perspective, cyber criminals will continue to attack our financial services sector, our information technology sector, and our manufacturing sector. From a security perspective, cyber terrorists will attack our critical infrastructure, including our energy sector, transportation network, water systems, and communication sector. As our societies and economies become more interconnected, they become both more efficient and more vulnerable to attack.

What role will the new college play in the realm of cybersecurity? Perhaps most importantly, we will be training students to understand the risks associated with cybersecurity. Every undergraduate student in the newly created minor in emergency preparedness, homeland security, and cybersecurity will be required to take a cybersecurity class. When the undergraduate major is approved, all students will take at least one introductory cybersecurity course and students will have the option to concentrate in cybersecurity within the major. When the new college creates graduate programs, we expect the cybersecurity program to be very popular. According to a recent article in Forbes, internet giant Cisco Systems reported that there are currently one million cybersecurity job openings around the globe; in the United States alone, there are 200,000 unfilled jobs (Forbes 2016). Moreover, most of these jobs require extensive academic training. The Burning Glass (2015) annual report on cybersecurity states that 84% of cybersecurity

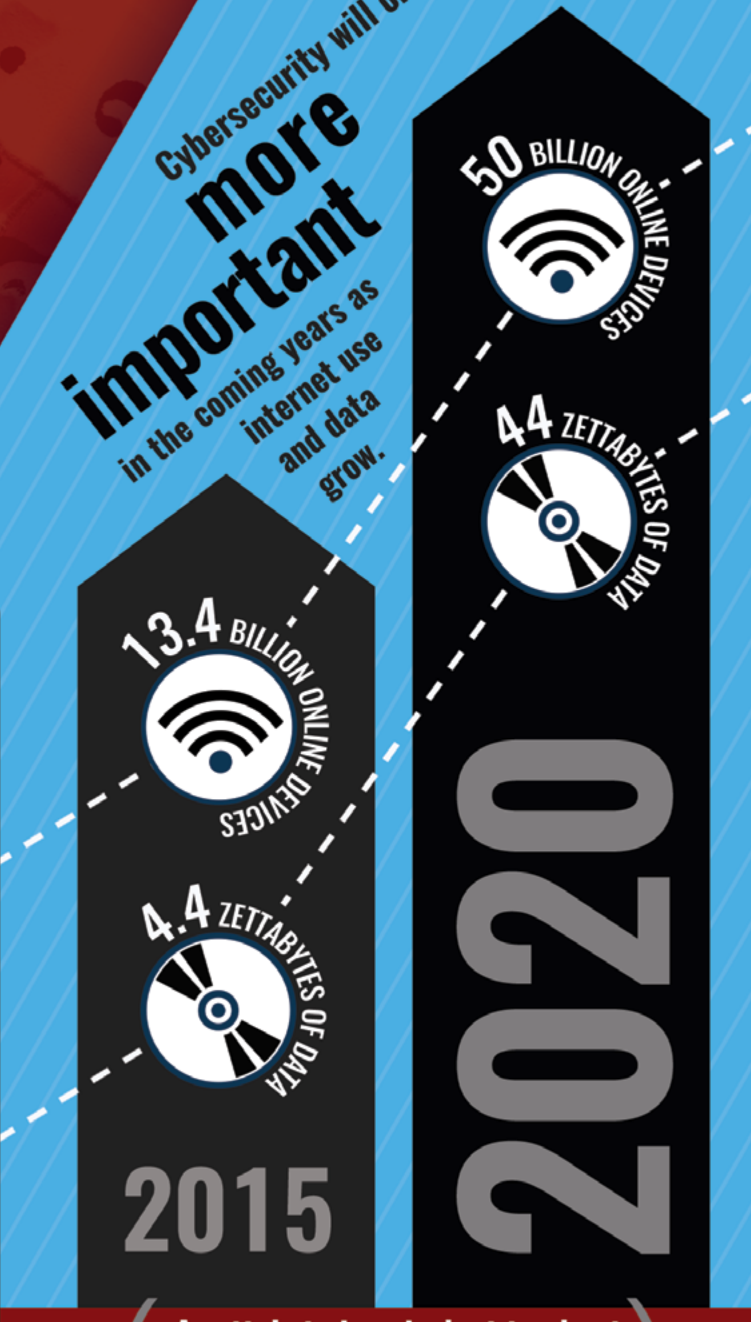
Continued on page 5

Did You Know?



Best Practices to Avoid Risks
Buy-in starts at the top
Enforce the rules
Train your users
Share responsibility with users

Cybersecurity will only become **more important** in the coming years as internet use and data grow.



A zettabyte is eqivalent to about **250 BILLION** DVDs

Most Common Passwords of 2015:

123456 abc123 password football qwerty

http://thehill.com/policy/cybersecurity/266325-most-common-password-in-2015-123456

AT&T Cybersecurity Insights: Decoding the Adversary, http://www.business.att.com/content/src/csi/decodingtheadversary.pdf

Cybersecurity Training: The Big Fail

Martin Manjak, CISSP, ISO
University at Albany

MARK SCHMIDT

Martin Manjak

Nearly every organization conducts fire drills involving their employees and facilities because they recognize how serious a threat fire can be, and because in many municipalities, they are required to do so by law. But even if fire drills were not mandated by statute, wouldn't you want your employees to know what to do in case of a fire?

Now consider the probability of a fire actually occurring in one of your sites, and compare that with the likelihood that one of your staff will be exposed to a digital threat. The fact is, US commercial, nonprofit, and government entities are subject to cyber-based attacks on a continuing, daily basis. Over half of Internet users receive at least one phishing e-mail per day[1]. Yet, how many organizations routinely train their staff on how to recognize and respond to such threats?

Fires are high impact, low likelihood events. They can be very destructive and result in loss of life, but thankfully, because of various code requirements and other controls, they are infrequent. Cyber intrusions and breaches, on the other hand, are both high in probability and impact, although they cannot result in physical harm (until those attacks target critical power, medical, automobile, or environmental controls).

According to statista.com, the US suffered $1.4B in direct property loss due to fire in 2014[2]. (This figure is limited to losses in the storage, industry, educational, and institutional property categories.) For many reasons, it's impossible to come up with an equivalent figure resulting from data breaches, but the partial numbers are still impressive. A report published by The Heritage Foundation stated: "A recent survey by the Ponemon Institute showed the average cost of cyber crime for U.S. retail stores more than doubled from 2013 to an annual average of $8.6 million per company in 2014."[3]

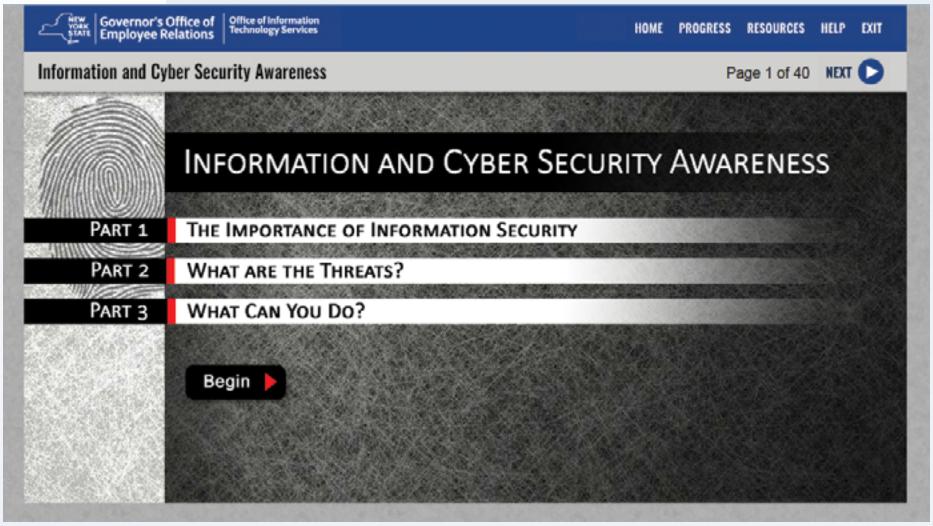
Despite the potential for significant loss and the prevalence of cyber-based attacks, how many organizations spend as much effort preparing their employees to respond to cyber threats as they do to the less likely event of a fire?

Continued on page 6

PDP Developing Web-Based Training: Information and Cyber Security Awareness

The Professional Development Program at Rockefeller College, University at Albany is currently developing a web-based module entitled Information and Cyber Security Awareness for the New York State workforce. When completed, this interactive course will feature three modules and take users about 60 minutes to complete. The course will discuss the importance of information security, describe the threats to information security, and provide learners with specific actions they can take to protect their agency's data.

Since 2006, PDP has developed six online trainings on cybersecurity for various state agencies. The speed at which technology evolves is evident when comparing course content over the years. For example, in 2006 learners were taught about the secure use of fax transmissions and the dangers of "internet e-mail." In 2016, faxes are almost non-existent and internet-based e-mail is the rule for most agencies. Additionally, in 2006 computer-based security measures were centered on desktop and laptop computers; in 2016, the use of personal devices, including smartphones and tablets, must also be considered as a source of vulnerabilities for security threats. These technology changes mirror the ongoing efforts to develop the effective training and policies needed to maintain adequate workforce response to such a complex and ever-changing issue. **PDP**



NEW YORK STATE
Governor's Office of Employee Relations
Office of Information Technology Services
HOME
PROGRESS
RESOURCES
HELP
EXIT
Page 1 of 40
NEXT
Begin

Information and Cyber Security Awareness

INFORMATION AND CYBER SECURITY AWARENESS

PART 1 THE IMPORTANCE OF INFORMATION SECURITY

PART 2 WHAT ARE THE THREATS?

PART 3 WHAT CAN YOU DO?

Information and Cyber Security Awareness e-Learning module created by the Professional Development Program, Instructional Technologies Unit

Effecting Cybersecurity: Integrating our Educational Defense is Key

Continued from page 1

to date seem inadequate to meet the threats occurring on an all-too-routine basis.

As a result of the clear and growing threat, a broader and stronger systemic approach is being explored as a solution. A key piece of that solution is the alignment of our education and training programs with the knowledge and best practices of experts in the field of cybersecurity. To accomplish this, specific steps are recommended:

1. Commitment from senior managers and leadership up to the CEO level; once leadership buy-in is secured, other critical action can move forward.
2. A broad survey of the policies, best practices, and trends of companies and organizations identified as leaders in cybersecurity, such as Cisco, Raytheon, AT&T, and the National Cybersecurity Center of Excellence; these programs, policies, and practices will serve as resources for developing learning objectives, training policies and practices, and curricula.
3. An analysis of the current state of knowledge, skill, and ability in the field of cybersecurity; the results will serve as data for building the body of knowledge needed to develop effective evidence-based learning for higher education curricula that will ensure a population of qualified graduates able to enter the field.
4. Needs analyses in specific organizations that identify the immediate task and work required for on-the-job success; this additional data will assist in developing the training programs to address immediate needs. Most likely non-technical staff will need general awareness and prevention training and more intensive technical training will be needed by IT staff. Successful training programs in this area will incorporate state-of-the art techniques, such as mock cyber-attack exercises that simulate deception, expose possible vulnerabilities, highlight additional learning needs, and provide feedback on training effectiveness in applying evidence-based findings to real-world challenges.

ED KIRCHGESSNER

Eugene Monaco

Cybersecurity is and will continue to be one of the most urgent issues facing our organizations. Since computer networks have historically been targets, organizations have been quick to take sensible precautions to minimize loss from those with criminal intent. By using the approach described above to establish the undergraduate and graduate degree programs, we will prepare those entering the field with the knowledge and the potential to have a constructive impact. In addition, the need remains for comprehensive and targeted evidence-based training and awareness programs in our workplace to defend against malicious or criminal activity. This approach is elaborated on by the articles of experts in this issue of the *Communiqué*. **PDP**

Educating and Arming the Next Generation of Cyberwarriors

Continued from page 2

job postings require at least a bachelor's degree. Our students will be in demand.

From a research perspective, there has been an explosion in funding for cybersecurity in the public, private, and nonprofit sectors. According to InfoSecurity Magazine, the global cybersecurity market will grow from $75 billion in 2015 to $170 billion in 2020. This year, President Barack Obama included $14 billion for cybersecurity efforts across the U.S. government to better protect federal and private networks from cyber attacks. The College of Emergency Preparedness, Homeland Security and Cybersecurity is currently seeking to hire innovative faculty researchers who can contribute to this global effort to combat cyber attacks.

Not a day seems to pass without the discovery of yet another cyber attack. Whether it is the private e-mail of the Director of National Intelligence, the U.S. Office of Personnel Management, or JPMorgan Chase, individuals and organizations are vulnerable to attack. While completely preventing intrusions is impossible, a skilled cyber workforce armed with tools from the best cyber research labs in the country and operating within sound security policies may be able to minimize the cost of breaches in the future. The College of Emergency Preparedness, Homeland Security and Cybersecurity hopes to be at the center of this effort. **PDP**

http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016

http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

http://www.businessinsider.com/us-government-cybersecurity-spending-2015-9

http://www.infosecurity-magazine.com/news/cybersecurity-spending-to-hit/

PDP *Communiqué* is produced by the Professional Development Program, Nelson A. Rockefeller College of Public Affairs and Policy, University at Albany, State University of New York.

Eugene J. Monaco
Executive Director and
Public Service Professor

Deanna Cooper, PhD
Editor

Jessica Bashaw
James Bonville
Mary Ellen Cox
Erica Hunter, PhD
Associate Editors

Ed Kirchgessner
Mark Schmidt
Photographers

Catherine Reynolds
Graphic Designer

Request an Electronic Version
Elect to receive the **Communiqué** via e-mail instead of print by making a request to: **newsletter@albany.edu.**

PDP

UNIVERSITY AT ALBANY
State University of New York

Professional Development Program
Rockefeller College, University at Albany
4 Tower Place
Albany, New York 12203

p (518) 442-6500; f (518) 442-6653
www.pdp.albany.edu

Cybersecurity Training: The Big Fail

Continued from page 4

What makes this situation even more astonishing is that your employees are far and away the weakest link in your organization's security controls. The most sophisticated defensive technologies can be easily circumvented by one curious employee clicking on a malicious e-mail link or attachment. In fact, the majority of major breaches suffered by government and commercial entities are the result of these types of social engineering attacks.

Do not underestimate your adversaries. The days of clumsy grammar and rampant misspellings that made it easy to identify fraudulent e-mail communications are gone. Today's cyber gangs are well-organized, well-funded, sophisticated, and highly motivated. They spend as much time as necessary researching their targets and can produce e-mail messages that are virtually indistinguishable from legitimate corporate communications. One organization estimated that 74% of internet users would download a potentially malicious file because they lack the "cyber-savviness" they need to spot dangers online.[4]

Organizations that do not prepare their employees for exposure to these attacks are failing at a fundamental level of due diligence. If you're not training your staff to recognize and respond to cyber threats, it's no less reckless than failing to protect them from a fire.[5] **PDP**

[1] http://www.phishing.org/

[2] http://www.statista.com/statistics/376639/us-fire-statistics-property-loss-due-to-fire-by-property-use/

[3] http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

[4] http://www.infosecurity-magazine.com/news/most-online-users-cant-spot-dodgy/

[5] http://www.infosec-cloud.com/security-awareness-training-the-numbers/