Volume 1, Issue 2

June 13, 2025

SOLUTIONS^3

Cyberside Chats: Summer Edition

Special points of interest:

- Critical patches across major platforms
- Massive cyberattack disrupts Whole Foods' sales
- Use strong, unique passwords for every account to boost security
- The rise of AI threats

Weekly Recap

Welcome to Week 2 of our Cybersecurity Internship Newsletter! As we wrap up week 2 here at Solutions^3, we kicked off the week with our weekly team-wide meeting where interns come together to set the stage for the week ahead, announcing important updates, current news in Cybersecurity, and projects for the week.

This week, interns collaborated together in group meetings to dive into the start of our first pathway, called the Cyber Essentials Pathway. This laid the foundation for key skills we worked on for our project deliverables this week. These sessions allowed interns to connect with each other, share insights, and work on creating a company of their choosing. Interns also met to discuss the structure and goals of the weekly newsletter, led by Bryan Montenegro this week.

A notable highlight was our vendor of the week session featuring Keatron Evans, the VP of Portfolio Product and AI Strategy at Infosec. Keatron Evans has over 20 years of experience in Cybersecurity and shared his expertise in Cybersecurity. Evans offered important career insights and held a questionnaire session where interns were able to ask insightful and thought-provoking questions regarding the evolving landscape of Cybersecurity as well as Infosec.

His perspective on current trends shaping the tech industry gave interns a valuable look into the industry as a whole and the future ahead of Cybersecurity.

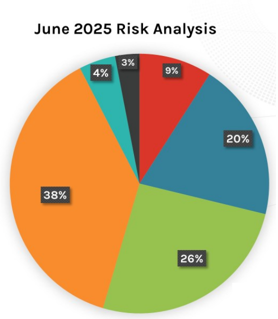
Inside this issue:

June's Critical Vulnerabilities	2
Major Food Distributor Shut Down	2
Stronger Passwords, Safer Accounts	2
Professional Development Recap	3
Deepfakes: The Future of Cyber threats?	3
Did You Know?	3
Editor's Corner	4

Vendor of the Week

This week, cybersecurity interns from Solutions^3 heard from Keatron Evans, VP of Portfolio and AI Strategy at **InfoSec Institute**. Drawing from his background in ground intelligence, Evans brought a valued perspective on evolving cyber threats, including malware command-and-control attacks and AI's rapid progression. He emphasized accessible communication in cybersecurity, stating, "Take something everyone can relate to and use that to get the technical point across." Interns gained insights on the importance of building practical skills instead of collecting certifications. Evans detailed InfoSec's approach- first designing practical exercises before building training around them. InfoSec's early pivot to online learning helped triple their business from 2020 to 2023, and they show no signs of slowing down in an age where protecting digital assets is crucial.

June's Critical Vulnerabilities: What You Need to Patch Now



Microsoft's June patches: RCE (38%) and Info Disclosure (26%) top risk types

This month's security headlines make one thing clear: vulnerabilities remain one of the biggest risks organizations face, and maintaining a disciplined patch process is one of the best ways to manage that risk. Across cloud, endpoint, and business-critical systems, a wave of serious software flaws surfaced, each capable of exposing sensitive data or disrupting operations.

Microsoft's June Patch Tuesday addressed 66 vulnerabilities, including an actively exploited zero-day in WebDAV and nine critical flaws, highlighting the need for timely OS and server updates. SAP's NetWeaver platform, used in enterprise ERP systems, was found to contain a flaw bypassing critical access controls, potentially exposing financial and HR data. Google also patched a widespread Chrome browser vulnerability that could deliver malicious code through everyday browsing, while a critical flaw in Roundcube webmail could allow remote takeover of email servers via a crafted message. Even endpoint defenses weren't spared, Trend Micro released June updates fixing weaknesses that could have allowed privilege escalation on protected devices.

This month's wave of critical vulnerabilities highlights the need for vulnerability management and incident response to operate as continuous, well-integrated processes, ensuring that when attackers outpace patches, organizations can detect, contain, and recover across every layer of their environments.

Cyberattack Shuts Down Major Food Distributor

United Natural Foods, Inc. (UNFI), one of the largest US grocery distributors and the primary distributor for Whole Foods, has been experiencing an ongoing cyberattack that has forced it to take its systems offline.

The company reported that they initially detected unusual activity on certain networks within their systems on June 5, 2025. They then decided to activate their incident response plan, which prompted them to take their systems offline.

While the nature of the breach has not been disclosed at this time, UNFI has since notified law enforcement to investigate the incident. This has not only significantly impacted their business operations, but also the company's ability to fulfil customer orders. The UNFI CEO, Sandy Douglas, has been in contact with their customers and suppliers, having transparent conversations to help manage the situation. In the meantime, UNFI is working diligently to restore its systems and review its security protocols.

> *"The threat actors out there are always looking for ways to innovate and find new ways to penetrate systems."*

Stronger Passwords, Safer Accounts

Are your passwords secure? Here are some quick tips to enhance your passwords and protect your accounts. Avoid using personal information such as birthdays, names, and locations as part of your password. Use a unique password for each account to minimize the amount of damage that can occur if one gets compromised.

If you are worried about having to memorize a ton of complex passwords, consider using a password manager that can generate and safely store strong, unique passwords for your accounts.

A strong password is a great first step, but why stop there? You can further protect your accounts by enabling two-factor authentication, which requires an additional form of verification to access your account, enhancing its security.

Professional Development Recap

The Solutions^3 Interns attended their second Professional Development session. This week focused on professionalism and workplace etiquette. Some learning objectives included demonstrating awareness of appropriate virtual and in-person workplace behavior, as well as understanding cultural norms, punctuality, accountability, and digital professionalism.

Interns then participated in an icebreaker activity in which they recalled a positive and negative impression they received in a professional setting. The activity got the group talking about how important first impressions are and how essential it is to present yourself in the best possible fashion.

Then, we learned about the four Ps of professionalism: punctuality, preparation, presence, and politeness. Shannon taught the interns about her sandwich method for giving constructive feedback, which follows the build, break, build methodology. Additionally, we spoke about the importance of body language and nonverbal cues. Shannon advised the group about professional conflict resolution and ways to combat unprofessional behavior from others.

Lastly, the group engaged in exercises to rewrite hypothetical unprofessional correspondence. Overall, the session was very informative and allowed the interns to further explore what it means to be a young professional in today's ever-changing professional landscape.

Deepfakes: The Future of Cyber Threats?

Imagine receiving a video of your company's CEO asking for an emergency wire transfer, only to later find out it was not real. This is one of the newest threats companies face today, thanks to Deepfakes.

Deepfakes describe AI-generated pictures, sounds, or videos that realistically portray people talking or acting in ways they never did. They can enable fraud, spread misinformation, and cause serious reputational damage.

As Deepfakes become increasingly sophisticated and accessible to attackers, awareness and training are crucial to reducing their impact. Organizations need to adopt a proactive approach to cybersecurity so they can protect themselves from these emerging threats.

To stay ahead, organizations should implement strict verification protocols for high-risk communications, train employees to recognize social engineering attacks, and adopt deepfake detection tools.

With Artificial technology advancing rapidly, how prepared is your organization to recognize and respond to this emerging threat?

> *"Deep fakes blur the line between truth and fiction like never before." – Neil deGrasse Tyson*

Did You Know?

In 2000, a mysterious email with the subject line "ILOVEYOU" spread quickly around the world. Only it wasn't a love letter - it was a computer virus known as the Love Bug. The virus disguised itself as a harmless file to trick users.

Once opened, the virus took over the victim's email, deleted files, and forwarded itself to all of their contacts. In just 24 hours, it infected more than 45 million computers and caused over $10 billion in damage. Businesses, governments, and individuals were all affected.

The Love Bug was a wake up call, showing how dangerous a simple email could be. It made people realize that cybersecurity isn't just about strong software - it's about awareness. One click led to global chaos.

Onel de Guzman—the 23-year-old responsible for the ILOVEYOU virus.

SOLUTIONS^3

637 Wyckoff Avenue
PMB 352
Wyckoff, NJ 07481

Phone: 201-891-0477
Fax: 201-891-5316
Email: info@solutions3llc.com

At Solutions^3 LLC, we believe that empowering people is the key to sustainable success in cybersecurity, IT, and business service management as a whole. Our commitment to resource development is evident through mentorships, advanced training, and workforce development programs, including impactful internships and apprenticeships.

For more information on our internships, workforce development, or training, contact Mike Battistella at mike@solutions3llc.com or Shannon Conley at shannon.conley@solutions3llc.com.

Special Thanks to Our Sponsors

We are grateful for the generous support and partnership of the following organizations, whose contributions help make the Summer Cybersecurity Internship Program possible. Their support enables us to provide hands-on learning experiences, real-world simulations, and invaluable mentorship opportunities for our interns.

DVMS Institute®

INFOSEC INSTITUTE

HACKTHEBOX

Follow us!

Website
www.solutions3llc.com

LinkedIn
www.linkedin.com/company/solutions3/

YouTube
www.youtube.com/@solutions3llc435

Editor's Corner

For this week, the interns at Solutions^3 were motivated and involved. From understanding appropriate work etiquette, to being able to learn from industry-leader Keatron Evans, this week focused on helping us build our fundamentals from the previous week.

This week was also the start of our pathway projects - these are capstone projects in which interns are divided into teams to focus on three major aspects of cybersecurity: cyber essentials, risk management, and incident response.

We began with cyber essentials, where we came together as a group to deliver a cybersecurity charter for a mock company to establish, test, and ensure the effectiveness of the company's cybersecurity policies. This helped us understand what companies must do in order to ensure maximum protection for their digital assets.

On a more personal note, I cannot express enough gratitude to the leadership team for the opportunities they are providing. Thank you for allowing us to network with industry leaders, teaching us the technical and business side of cybersecurity, and serving as great mentors.

Lastly, I want to thank Julia, Andre, Aaron, Dominick, John, Jaylen, Amaan, and Jesus for their work in this issue of the newsletter. I'm thrilled to have them as my fellow interns, and even more thrilled to show everyone what we are working on throughout the summer!

— Bryan Montenegro
M.S. Computer Science, Felician University