Volume 1, Issue 3

June 20, 2025

SOLUTIONS³

Cyberside Chats: Summer Edition

Weekly Recap

Special points of interest:

- The aftermath of United Natural Foods Cyberattack
- Cyberattack hits Washington Post journalists covering national stories
- INTERPOL's Operation Secure dismantles over 20,000 malicious IPs and domains
- Emerging ransomware to look out for

Welcome to the 3rd issue of our Cybersecurity Internship Newsletter, highlighting key moments from this week's program! As we wrap up Week 3 at Solutions³ LLC, we kicked off the week with our regular start meeting to align on goals and build on the momentum from a strong Week 2. This week marked the second phase of our Cyber Essentials Pathway, which provided a deeper technical foundation to support our upcoming project deliverables. Interns worked in teams to further develop Falconi, our mock NFL sports agency, applying cybersecurity concepts in a hands-on, collaborative setting. Each group focused on identifying assets, implementing access controls, and creating policies essential for securing organizational systems and assets

In addition to the pathway project, interns also collaborated on this week's newsletter, led by Dominick Battinelli.

A highlight from Week 3 was the Professional Development session with Kristen Nova which focused on effective communication strategies. The interns learned how to clearly explain complex technical ideas to both technical and non-technical audiences.

Another highlight of the week was our Vendor of the Week session with Floyd Hanes, Solutions Engineer II, and Chandler Anderson, Senior Account Executive - SLED, from Hack The Box. Their insight, enthusiasm, and support energized us for the upcoming Hack The Box challenges, creating an engaging and motivating environment for everyone involved.

Vendor of the Week

This week, interns at Solutions³ met with Floyd Haynes and Chandler Anderson from **Hack the Box**. Floyd, a retired 21-year Air Force veteran, is a Solutions Engineer specializing in threat emulation and cyber forensics. Chandler, a former furniture sales representative, now serves as a Senior Account Executive managing client relations. They highlighted Hack the Box's value as a gamified, hands-on platform that builds skills from cybersecurity basics to advanced threat scenarios. When asked about key skills interns should develop, Floyd emphasized that "consistency is key" for continuous learning, while Chandler stressed soft skills and the power of asking questions to better understand your audience. Interns will continue working with both professionals through weekly Hack the Box sessions to develop their cybersecurity knowledge and practical skills.

Cybercrime Starves Shelves Nationwide in the Aftermath of the United Natural Foods Attack

This week, a major cyberattack on United Natural Foods, Inc. (UNFI), one of the nation's largest food distributors, has led to empty shelves in grocery stores nationwide. UNFI detected unauthorized activity that entered its IT systems last week, prompting the company to shut down its network to contain the breach. This resulted in many supermarkets experiencing shortages, especially for essential food items such as milk, pasta, and frozen items. UNFI is a major distributor for retail giant Whole Foods, which distributes to over 30,000 stores nationwide.

UNFI's CEO, Sandy Douglas, explained in a video message that the company is working hard to restore operations to normal by the end of the weekend. Currently, stores have begun posting signs apologizing to customers for out-of-stock items, which are pushing stores to find alternative suppliers. Linda Gommel, the CEO of Lucerne Valley, is turning to other companies to fulfill stop-gap orders.

This disruption truly highlights the vulnerabilities in the food supply chain industry and the long-term impact of cyberattacks on critical infrastructure. UNFI continues to work toward resolving the outage to ensure customers can access their essential items ahead of the weekend.

Washington Post Cyberattack

"A breach like this isn't just an IT issue. It's a threat to democracy"

On June 12, The Washington Post discovered a cyberattack that compromised the email accounts of several journalists. The breach affected Microsoft email accounts and seemed to target journalists covering national security and China. The attack is believed to be the work of a foreign government or actors seeking extortion. As mitigation, the Post enforced employee password resets as well as credential resets. Additional systems and customer data do not appear to be among the impacted assets.

According to employees at the company, sensitive information is usually discussed through mediums such as Slack and Signal, as opposed to email. A similar incident affected News Corp in 2022, in which hackers targeted Wall Street Journal reporters who were covering matters relating to China. While The Washington Post hasn't released many specifics yet, the implications are clear. A breach like this isn't just an IT issue. It's a threat to democracy.

Success of INTERPOL's Operation Secure

INTERPOL's Operation Secure was a coordinated effort of over twenty-six nations throughout Asia and South Pacific, conducted between January and April 2025. The goal of the operation was to target malicious information stealing cyber threats. The effort was highly successful in that they seized 41 servers, seized over 100 GB of malicious data, took down over 20,000 IPs and domains, arrested 32 people, and notified over 215,000 victims. Additionally, they confiscated over $10,000 in cash, SIM cards, and business registration documents. INTERPOL collaborated with private sector cyber organizations, including Group-IB and Trend Micro, to locate servers, map physical networks, and identify the infostealers. The organized raid underscores INTERPOL's commitment to collaborative action in combating global cybercrime.

Professional Development Recap

This week's professional development session centered on the importance of clear and effective communication in the workplace, an essential skill across every field. Interns explored how to effectively deliver their message across verbal, written, and nonverbal forms of communication.

The session featured interactive activities that challenged us to simplify technical topics for non-technical audiences, tailor messages to different stakeholders, and develop concise reporting skills. After each activity, Kristen provided constructive feedback on what we did well and where we could improve. A key takeaway from this session was the value of preparing and organizing our thoughts beforehand to minimize filler words, as these can weaken the impact of the message. Effective communication isn't just about speaking, it's about ensuring your message lands clearly and purposefully.

In cybersecurity, strong communication skills are critical. Any delay or confusion during an incident can lead to greater damage. Effective communication builds trust, enhances teamwork, and ultimately helps protect systems.

The Ransomware That Doesn't Care If You Pay

In the world of cybersecurity, a ransomware strain known as Anubis is raising major concerns. Unlike most ransomware that locks files until a ransom is paid, Anubis goes further by permanently erasing the data inside them. The file names and folders may remain, but the content is gone for good.

Anubis has an integrated function called "wipe mode," which can be activated by a particular command. By combining file encryption with permanent data wiping, it increases pressure on victims and makes it clear that paying the ransom will not restore their files. Targeted industries include healthcare, construction, and education.

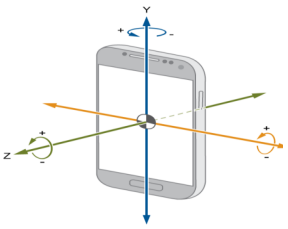
Ransomware tactics are changing, with an emphasis on more destruction rather than profit. It serves as a reminder to have reliable backups, secure devices, and caution when clicking on suspicious links or emails. The best way to stay safe is to stay prepared!

"Ransomware is more about manipulating vulnerabilities in human psychology than the adversary's technological sophistication." — James Scott, ICIT Fellow Senior

Did You Know?

Your phone's motion sensors, like the ones that detect tilts and shakes, can quietly give away your passcode. A technique called PINLogger.js uses simple website code to track how your phone moves when you tap the screen. With that data, it can guess a 4-digit PIN with up to 74% accuracy, even if your screen is off. While newer phones and browsers have added protections, older devices and shady apps can still be vulnerable. Even visiting the wrong page could put your lock screen at risk, so be mindful of where you tap. To stay safe, keep your device updated, limit sensor access for apps and websites, and avoid clicking unfamiliar links—because sometimes, your phone's sensors know more than you think.

Cybercriminals don't always need direct access to your data—sometimes, they just need you to tap in the wrong place at the wrong time. Stay alert!



637 Wyckoff Avenue
PMB 352
Wyckoff, NJ 07481

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

At Solutions³ 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.

Follow us!

Website
www.solutions3llc.com

LinkedIn
www.linkedin.com/company/solutions3/

YouTube
www.youtube.com/@solutions3llc435

Editor's Corner

In this week's issue of Cyberside Chats, we showcase the ever-evolving nature of cybersecurity and its critical importance across all industries. From an attack on Whole Foods' supply chain, the evolution of ransomware attacks, and targeted strikes on journalists' email accounts, it's clear that cybersecurity is a fundamental business priority. Every organization, regardless of size or sector, must take proactive steps to protect its digital assets in this rapidly changing landscape.

Entering week 2 of the Cyber Essentials pathway, us interns have continued building out the cybersecurity framework for our fictional sports management company, Falconi. We identified our digital assets, visualized our infrastructure and implemented access control policies to safeguard key assets. We also met with Floyd Haynes and Chandler Anderson from Hack the Box who we're thrilled to be working with for the rest of this internship. All of us interns are looking forward to the weekly Hack the Box sessions including two Capture the Flag competitions.

To round out this issue, I want to give a big thanks to the leadership team at Solutions³ for their mentorship, enthusiasm, and continued support. I also want to express my gratitude to my fellow interns who all came together to make this issue of Cyberside Chats possible. We are excited to continue sharing our journey throughout the summer!
— Dominick Battinelli
M.S. Cybersecurity, Stevens Institute of Technology