Volume 1, Issue 5

July 3, 2025

SOLUTIONS3

Cyberside Chats: Summer Edition

Special points of interest:

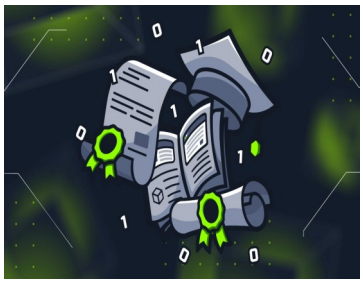
- Ahold Delhaize Data Breach
- FBI's New Warning on Social Engineering Attacks
- Why Cybersecurity Should Come Before AI in Schools
- Hawaiian aviation sector faces major cyber attacks

Weekly Recap

This week, interns progressed into the Incident Response pathway, focusing on foundational concepts in information security and structured response processes. As part of this transition, they completed an InfoSec training module on the incident response lifecycle and began new Hack the Box modules designed to reinforce technical skills through hands-on learning. This gave interns an in-depth look at what Hack the Box has to offer.

Tuesday's professional development session, led by Shannon, focused on time management and prioritization. Interns explored frameworks like the Eisenhower Matrix and participated in reflective activities such as "What Stole Your Time?" to identify habits that impact productivity and learn strategies for managing competing demands.

Throughout the week, interns met with Kristen to review deliverable progress and ensure coordination across teams. They also joined a Hack the Box session facilitated by Floyd Haynes, Solutions Engineer II, who provided a walkthrough of a SOC environment and led a discussion around individual cybersecurity interests. These activities supported both technical development and soft skill growth, helping interns apply new knowledge within the broader context of their Incident Response work.



Inside this issue:

Vendor of the Week

This week marked the first Power Hour with Hack the Box and a great opportunity to speak with Floyd Haynes about the training modules completed. Interns had an engaging discussion on red vs. blue team roles. With many having blue team experience, interns expressed interest in exploring red teams offensive strategy.

Interns noted blue team roles felt more high stakes with the consequences of failure. Floyd emphasized failure is subjective and part of the learning process. He reminded us: "Nobody is 100% safe. Incidents will happen. Be reactive and handle them."

Finally, Floyd walked us through his SOC's workflow including threat hunting, malware analysis, and cyber threat emulation. Interns walked away with a deeper understanding of both offensive and defensive strategies in cybersecurity.

Ahold Delhaize Data Breach

The grocery and retail sector continues to face escalating cyber threats. Last week, Ahold Delhaize, the parent company of Giant Food, Food Lion, Hannaford, Stop & Shop, and other major U.S. supermarket chains confirmed that a ransomware attack in November of last year resulted in a data breach impacting over 2.24 million individuals.

The Inc Ransom group has since claimed responsibility for the attack, stating they exfiltrated over 6 terabytes of sensitive data, 800 gigabytes of which they have already leaked online. The breach exposed employment records and customer data including names, social security numbers, and contact information.

The attack was first detected in November 2024, when several Ahold Delhaize owned pharmacies experienced system outages. In the months since, forensic analysis revealed that the attackers were able to access internal systems, and targeted employee data across multiple business units.

Ahold Delhaize is offering two years of free credit monitoring and identity protection to affected individuals, but this incident highlights growing concerns across the retail industry. As ransomware groups evolve their tactics, organizations must stay vigilant and stay secure.

FBI Issues New Warning against Expanding Social Engineering Attacks

"The true danger of social engineering techniques is that people's emotions and fears are preyed on, then weaponized for further harm"

The FBI has alerted the public to remain vigilant as the notorious cybercrime group, Scattered Spider, ramps up their attacks. While the group is most known to target third-party IT providers to gain access to large organizations, they are becoming more reliant on social engineering to gain access into secure systems. Social engineering refers to the intentional deception by bad actors to manipulate victims into giving them confidential or personal information for the purpose of being exploited by the bad actor. Google subsidiary, Mandiant, has additionally alerted of Scattered Spider's targeting of the insurance sector as well as the airline and transportation industries. The true danger of social engineering techniques is that people's emotions and fears are preyed on, then weaponized for further harm. These attacks are not of brute force or high technical savvy; they are perfectly crafted to stress out victims to reveal valuable information.

Why Cybersecurity Should Come Before AI in Schools

AI is quickly becoming a staple in classrooms, helping students process complex subjects and allowing teachers to simplify difficult concepts. While this shift is beneficial, there is a growing concern that students are not receiving enough education on cybersecurity. Introducing AI without first teaching cybersecurity creates serious risks. Without foundational knowledge, students may struggle to recognize threats like phishing, data breaches, or misinformation. Since children begin using technology at a young age, it is crucial that they also learn how to stay safe online. Teaching cybersecurity basics early can improve critical thinking skills, promote safer internet habits, and prepare students for the future of technology. Cybersecurity should be treated as a core subject, not an afterthought to AI.

Professional Development Recap

For this week's professional development session, hosted by Shannon and Kristen, the interns learned how to master time management and efficiently prioritize tasks when the going gets tough.

Especially in the workplace, there will be times when everything feels urgent, and if these situations are approached incorrectly, they can lead to an individual feeling highly stressed and burnt out. Through practical discussion and examples, the interns explored how to prioritize tasks by measuring their urgency and importance. This was possible through the use of prioritization techniques such as the ABC Prioritization Method and the Eisenhower Matrix. With the supplement of time-blocking techniques, involving the use of reminder and calendar apps, these strategies gave interns practical ways to manage their days and stay focused. The interns also tackled the Cyber Task Triage Challenge, where they split into groups to quickly categorize real-world cybersecurity tasks by priority.

As the session came to a close with personal reflection, the interns shared small habits they intend to change and identified their biggest time-wasters. They ultimately learned that time management is not about doing as much as one physically can. It's about focusing first on the tasks that make the biggest impact.

Hawaiian Airlines: Aviation Industry Targeted

Following WestJet's cybersecurity incident of June 13, another airline became targeted: Hawaiian airlines. On June 26, Hawaiian airlines reported a disruption to their IT systems to the FAA. The nature of the attack itself has not been disclosed, but reports suggest it to be a ransomware attack for monetary compensation. Alaska Air Group, owner of Hawaiian airlines, reported that the attack did not disrupt service operations or flights, but they are working to bolster their security.

This is the latest airline targeted in three months, and the FBI has warned airlines of the most likely perpetrators: the cybercriminal group known as the Scattered Spider. The Scattered Spider is a community of hackers credited with many high-profile cyber attacks, in which they use social engineering, phishing, and SIM swapping to bypass security. North American airlines are now on high alert, setting up preemptive measures to counter the Scattered Spider.

In a lot of cases, they'll move laterally and search for a cyber insurance plan or an incident response plan or a breakdown of the company's financials as a way of assessing their demand." – Alex Waintraub, a cyber crisis management expert at CYGNVS

Did You Know?

While hacking is typically associated with computers and IT systems, today's cars are increasingly vulnerable to cyber threats. Modern vehicles rely on software and internet-connected features that can be exploited. A recent flaw in Subaru's Starlink system allowed hackers to access key functions, such as remote start and GPS tracking, using only a license plate and basic owner info. In some cases, weak manufacturer apps have let outsiders control other users' vehicles. To reduce risk, automakers must prioritize regular security updates and stronger encryption. Drivers can also protect themselves by using strong passwords, enabling two-factor authentication, and disabling unused features. As cars become more connected, cybersecurity is no longer optional- it's essential.

"As cars become more connected, cybersecurity is no longer optional- it's essential."

SOLUTIONS³

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

This week, interns began the Incident Response pathway, exploring how critical incident handling is for organizations. Our main deliverable was building an IR team for our mock company, Falconi, a sports management agency we've developed throughout the internship. With support from Hack the Box and Floyd Haynes, we were introduced to key concepts in information security and IR handling through interactive modules.

We also participated in a Power Hour with Floyd Haynes and Chandler Anderson from Hack the Box, discussing lessons learned and insights from the platform. Excitement continues to grow as we dive deeper into this pathway.

One of the most rewarding parts of this journey has been collaborating with our intern team, who bring such creativity, insight, and energy to the table. A special thank you to Aaron, Amaan, Andre, Bryan, Dominick, Jesus, Jonathan, and Julia—it's been a pleasure learning and growing alongside you all, and I'm so grateful to be on this journey with you all.

As we close out Week 5, I want to thank our incredible leadership team for their mentorship and unwavering support. I am looking forward to where the next few weeks take us. And that wraps up Week 5 of the Solutions3 internship. Thank you to all my fellow interns and the team at Solutions3 for making this edition of cyberchats possible as we share our journey.

~ Jaylen Weerasinghe