Monthly Cybersecurity Newsletter

May 2024

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Torry Crass

May 13-17 Is Business Continuity & Resilience Awareness Week

Business Continuity & Resilience Awareness Week (May 13-17) is The Business Continuity Institute's most popular campaign that raises awareness of business continuity and resilience. The campaign offers free access to professionals and organizations across all industry sectors to a wide range of resources covering business continuity and resilience, as well as related disciplines.

BCAW+R 2024 will feature the theme "Empowering Tomorrow: Building Resilience Today" and will cover different areas of the resilience discipline, which are also a key focus on many of the disruptive events currently happening.

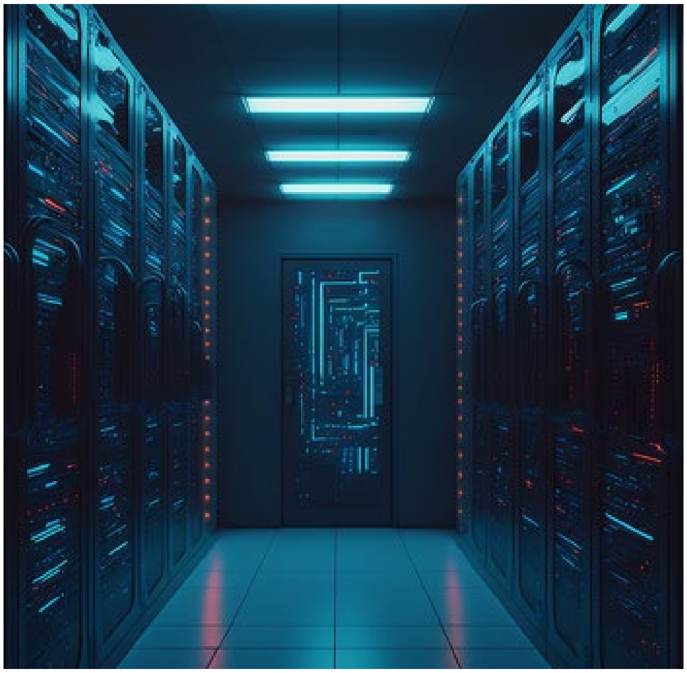
Each day of the week – from 1-1:30 p.m. – the N.C. Department of Information Technology's Enterprise Security and Risk Management Office, along with N.C. Business Continuity Team partners, will be presenting a 30-minute "Business Continuity Talk."

The discussions will revolve around the resilience discipline being highlighted that day in relation to business continuity from a state government perspective.

Please plan on joining each day via Teams to explore these short educational opportunities pertaining to Resilience. Contact BCM@nc.gov for more information.

Day	Topic	Presenter
Monday, May 13	Proactive Preparedness	**Torry Crass**, *State Chief Risk Officer* NCDIT Enterprise Security & Risk Management Office
Tuesday, May 14	Building Community Resilience	**Samantha Royster**, *NC CERT Program Manager* N.C. Emergency Management
Wednesday, May 15	Employee Engagement and Aligning with DEI, Environmental and Social Responsibility	**Dr. Katina Blue**, *Associate Vice Chancellor/Chief Information Officer* University of North Carolina at Pembroke
Thursday, May 16	Learning from the Past and Preparing for the Future	**Albert Moore**, *IT Security and Compliance Specialist* NCDIT Enterprise Security & Risk Management Office
Friday, May 17	Resilience and Innovation	**Keith Briggs**, *Enterprise Architecture & Innovation Director* **Justin Vargas**, *Intelligent Automation Architect* NCDIT Enterprise Architecture & Innovation

System Shutdown: Cyberattack on America’s Largest Healthcare Payment Processor



The recent cyberattack on Change Healthcare, a key player in the U.S. healthcare payment system, has led to significant disruptions in healthcare services and financial transactions across the country.

The attack, which began on Feb. 21, has had an impact on a wide range of healthcare operations – from pharmacies being unable to process prescriptions to hospitals facing severe cash flow challenges.

As a result, many healthcare providers are struggling to make payroll and cover other critical operating expenses.

Change Healthcare, which processes approximately 15 billion healthcare transactions annually, plays a crucial role in the verification of eligibility, pharmacy operations and the transmission of claims and payments. The disruption has severed the digital link between providers and insurers, delaying millions of dollars in payments and exacerbating the operational challenges in healthcare facilities.

The response to the crisis has been multifaceted.

The U.S. Department of Health and Human Services (HHS) has been actively involved, urging other payers in the healthcare system to assist by making interim payments and reducing administrative burdens on providers.

HHS has also encouraged Medicare Administrative Contractors to expedite processes for providers needing to switch clearinghouses to continue billing electronically. HHS has also advocated for the relaxation of prior authorization and other utilization management requirements during this period.

Despite these measures, there has been criticism from within the healthcare sector regarding the adequacy of the response, with calls for more direct and effective interventions to address the urgent needs of the affected healthcare providers.

In addition to immediate responses, there's a broader push from government and industry stakeholders to strengthen cybersecurity resilience within the healthcare sector to prevent such significant disruptions in the future. This includes a greater emphasis on cybersecurity best practices and preparedness across the healthcare ecosystem to protect against similar attacks.

The ongoing impact of the cyberattack and the responses from various sectors highlight the critical importance of cybersecurity and the need for robust, coordinated action to safeguard essential healthcare services against emerging digital threats.

Identifying Fraud: How the U.S. Postal Service Became the Top Target for Phishing Fraudsters

The U.S. Postal Service has emerged as the most impersonated brand in phishing attacks, highlighting a significant cyberthreat that exploits public trust in this widely recognized institution.

Phishing campaigns cleverly designed to mimic USPS communications are increasingly common, as cybercriminals target individuals with emails and texts that purport to be from the postal service.

These phishing attacks often involve messages claiming issues with package delivery, tracking updates or urgent notices requiring immediate action, such as confirming personal information or making a payment to release a parcel.

These messages typically contain malicious links that, when clicked, can lead to the installation of malware on the victim's device or direct them to a fraudulent website designed to steal personal information.

The choice of USPS as a facade for phishing schemes is strategic. The postal service's broad customer base and the public's routine interaction with its services make it a likely guise for scams.

Most consumers expect regular communication from USPS and are therefore less suspicious of emails and messages they believe are from the postal service. This familiarity breeds a dangerous complacency, making the scams more effective.

To protect themselves, experts recommend that individuals be vigilant and scrutinize emails and text messages that claim to be from USPS. Key red flags include:

- Generic greetings
- Grammatical errors
- Urgent and unsolicited requests for personal information
- Payment demands
- Links to unfamiliar websites

USPS has consistently advised that they do not send unsolicited requests for personal or financial information via email.

Organizations like the Federal Trade Commission and cybersecurity firms regularly update the public on how to recognize and avoid such phishing attempts. For more effective prevention, it is suggested that individuals directly navigate to the official USPS website or contact USPS customer service directly when they receive suspicious communications come from the postal service.

The rise of USPS impersonation in phishing attacks underscores the need for continuous public education on cybersecurity practices and the importance of critical evaluation of all electronic communications, particularly those that involve sensitive personal data.

The Crucial Role of Cybersecurity in Protecting Clean Energy Infrastructures

As we move toward more sustainable energy sources, clean energy – in conjunction with cybersecurity – is becoming more crucial. The promising reliance on digital technologies in clean energy infrastructures – from smart grids to renewable energy sources like wind and solar – brings a heightened risk of cyberthreats. Ensuring the resilience of these energy systems against cyberattacks is vital not only for maintaining energy security but also for the ongoing transition to cleaner energy solutions.

Modern clean energy systems are integrated with advanced technologies that allow for remote monitoring, real-time data analytics and automation. While these technologies enable more efficient management of energy resources, they also expose the systems to potential cyberthreats.

For example, smart grids use information and communication technologies to manage electricity flow, which can be disrupted by cyberattacks aimed at destabilizing the grid. Renewable energy sources, like solar panels and wind turbines, rely on interconnected systems that, if hacked, could lead to significant outages and financial losses.

A successful cyberattack on the clean energy infrastructure could have far-reaching consequences. Besides the immediate disruption of energy supply, such attacks could undermine public confidence in renewable energy technologies, potentially slowing down investment and adoption rates.

Moreover, as countries increase their reliance on renewable sources to achieve carbon neutrality, the strategic importance of securing these energy systems from cyberthreats becomes even more significant.

The future of clean energy is not only a question of technological innovation and policy support but also of ensuring that these technologies can withstand the evolving landscape of cyberthreats. As the clean energy sector continues to grow, integrating robust cybersecurity practices will be essential.

By doing so, we can safeguard our sustainable energy future and ensure that clean energy technologies continue to provide reliable, safe, and efficient power to meet global needs. This holistic approach to cybersecurity is crucial for the stability and success of the global shift towards renewable energy sources.

Securing Automated Vehicles: A Tesla Case Study

The unveiling of Tesla's Cybertruck, an innovative addition to the electric vehicle market, is turning heads due to its unique design. It is also raising important questions about cybersecurity in the era of automated vehicles.

As Tesla pushes the envelope with its creativity of computerized features and connectivity, the Cybertruck emerges as a case study of how the process of securing these modernized vehicles are affected.

A recent recall of the Cybertruck, due to faulty accelerator pedals, prompted immediate safety and security concerns with the vehicle's software system as noted by safety professionals.

This sophisticated system controls everything from the electric powertrain to autopilot functionalities and is integral to the vehicle's performance and overall safety. The system's complexity alone introduces significant vulnerabilities.

Malicious actors targeting these systems could potentially hijack vehicle controls or disable critical safety features. Tesla addresses these risks through rigorous encryption and regular over-the-air software updates, which promptly patch identified vulnerabilities.

Tesla vehicles collect extensive data to enhance performance and user experience, including real-time location tracking, driver behavior analytics and vehicle usage statistics. This trove of data, if mishandled, could lead to serious privacy breaches.

Tesla has historically been proactive about its cybersecurity, employing a dedicated security team and running a public bug bounty program that gives incentives to security researchers with the hopes of identifying and reporting vulnerabilities.

Such initiatives are crucial for the Cybertruck, as they help the company stay ahead of potential cyberthreats. As Tesla continues to innovate, its commitment to cybersecurity will be just as important as the features it introduces.

Data Breach at United Healthcare: A Third of American Data Potentially Compromised

United Healthcare, one of the largest health insurers in the United States, has reported a significant data breach that potentially impacts a third of the American population.

The breach was first detected earlier this year when unusual activity was noticed on United Healthcare's digital platforms. Investigations suggest that sophisticated hackers, possibly part of an organized cybercrime group, exploited vulnerabilities in the system to gain unauthorized access to an array of personal information.

The data accessed includes sensitive personal information such as Social Security numbers, medical records and financial details. This type of information is extremely valuable on the black market, potentially exposing affected individuals to identity theft and financial fraud.

United Healthcare has responded to the breach by engaging leading cybersecurity experts to contain the situation and enhance its security measures. The company is also cooperating with law enforcement agencies to trace the source of the attack and mitigate future risks.

Affected individuals are being notified and offered credit monitoring and identity protection services. This incident raises serious concerns about the security measures in place at major healthcare providers and the potential risks to personal privacy.

The breach at United Healthcare serves as a wake-up call for the healthcare industry, highlighting the need for stringent cybersecurity measures. Healthcare providers hold some of the most sensitive personal data, making them prime targets for cybercriminals. As investigations continue, the full extent of the breach and its repercussions will become clearer, potentially leading to significant changes in the industry's approach to data security.

Training & Continued Learning Resources

- FedVTE: Free Online Training Environment: https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service: https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies: https://niccs.cisa.gov/
- ICS-CERT Training: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Cybersecurity Newsletters

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4. Access the newsletter. ***Note:*** *You must have a valid state employee Microsoft 365 account.*

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security. https://www.cisecurity.org/insights/newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

Upcoming Training & Events

May 8: SANS Webinar: Combatting Crypto Miners: Tailored Incident Response for Azure, AWS, and Google Cloud

May 8: SANS Webinar: Next-Generation Microsoft 365 Logging: Exploring New Features

May 13-17: Business Continuity & Resilience Awareness Week

May 13: SANS Webinar: How to Prevent Social Engineering based on Successful Red Team Exercises

May 16: SANS Webinar: Prevent Remote Code Execution with Private Endpoints – Aviata Solo Flight Challenge Chapter 2

May 20: SANS Webinar: Exploring the Link Between Corruption and Cybercrime

May 23: SANS Webinar: Resilient by Design: Rethinking Cybersecurity in Manufacturing

View a list of upcoming SANS webcasts.

Be sure to follow the N.C. Department of Information Technology on X (formerly known as Twitter), Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. Remember … Stop. Think. Connect.

Disclaimer: Vendors, references and links in this newsletter are for informational purposes only, and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.