Business Continuity and Resilience Awareness Week: NCDIT to Host Webinars on Empowering Resilience with AI

May 19-23 is Business Continuity and Awareness WeeBusiness Continuity and Resilience Awareness Week (BCAW+R), and the N.C. Department of Information Technology invites you to join a series of five webinars on Empowering Resilience with AI.

Business Continuity Awareness Week is an annual international technology initiative to raise awareness of the importance of establishing a solid infrastructure that can withstand all sorts of damages and interruptions to an organization's business operations.

Learn from NCDIT and national experts on how to leverage AI to predict potential disruptions to your organization's work and provide vital services if any interruptions occur.

Explore how to proactively incorporate new technologies to build a solid, resilient infrastructure.

Who Should Attend

Anyone with a role in ensuring their organization's ability to continue functioning well amid potential disruptions should attend.

That includes:

- Chief information officers
- Security liaisons
- IT staff

BCAW+R Featured Speakers

The webinars will take place each day on Microsoft Teams at 1-1:30 p.m. May 19-23. **Click on the link for each webinar to join.**

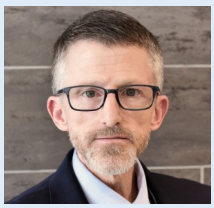
May 19
Predictive Analytics and Forecasting
I-Sah Hsieh
AI Governance and Policy Executive, NCDIT

May 20
AI & Exercises
Timothy Davis
Lead Cyber Threat Intelligence Analyst, Center for Internet Security

May 21
Supply Chain & Cyber Resilience
Teena Piccione
NCDIT Secretary and State Chief Information Officer

BCAW+R Featured Speakers

May 22
Embracing Organizational Resilience Through AI
Bernice Bond
Chief Information Security Officer, NCDIT



May 23
Success Stories Showcasing AI Applications Across Industries
Keith Briggs
State Chief Architect and Innovation Director, NCDIT

Also speaking on May 23

Justin Vargas
AI Architect, NCDIT

Backups Become the Focus as Ransomware Attacks Target Three-Fourths of Organizations

New data puts the spotlight on how most organizations are unable to completely recover their data after a ransomware attack, making the case for better data protection for improved incident response.

Organizations simply don't appear to be prepared in for ransomware attacks, according to backup vendor Veeam's just-released 2022 Data Protection Trends Report.

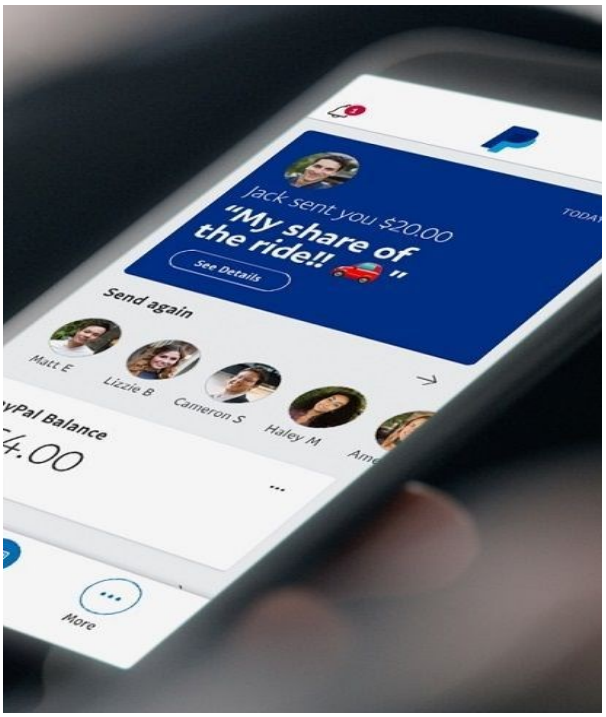
Most organizations have a less-than-perfect ability to recover from major business disruptions. According to the report, ransomware specifically is a huge problem for organizations today:

- 76% of organizations experienced a ransomware attack in the past 12 months.
- 60% of organizations experienced two or more attacks in the same timeframe.
- At best, only 80% of the data was recoverable – and only 19% of organizations could recover that.
- The organization is only able to recover about 64% of its data on average.

This says a lot about how your organization should be approaching its response to ransomware – and even about preventive measures to stop attacks before they have an impact.

With most organizations unable to fully recover and the majority facing attacks, organizations can do a few things right now:

- **Think disaster recovery, no backups.** Have the ability to fully recover some or all of your environment after a ransomware attack. That means you've got a full disaster recovery plan in place, complete with a recovery team, simulation testing, a communication plan, etc.
- **Improve security at your weakest point.** Veeam's report also notes that 42% of the ransomware attacks on those organizations started with a user who clicked on a malicious link. That means, despite all the security solutions in place, malicious emails are still getting through. So, it's up to the user receiving the email to stop the attack by recognizing the phishing email and choosing not to engage with it.



This is what Security Awareness Training teaches users: stay vigilant, play a role in organizational cybersecurity, and stay clear of suspicious or malicious content in emails or on the web.

This article is redistributed with permission from KnowBe4.

Training & Continuing Learning Resources

TEEX: Texas Engineering Extension Service:

https://teex.org

NICCS: Free Online Training Environment:

https;//niccs.gov/education-training/cisa-learning

NICCS: National Initiative for Cybersecurity Careers & Studies:

https://niccs.cisa.gov

ICS-CERT Training:

https;//www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa

Additional Cybersecurity Newsletters

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

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

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.*