SHARE:

BLOG

The Power of Resilience

What America can learn from our partners in Ukraine

Released: August 09, 2023

Jen Easterly, Director Cybersecurity and Infrastructure Security Agency

Victor Zhora, Deputy Chairman and Chief Digital Transformation Officer of the State Service of Special Communication and Information Protection

In the late afternoon of December 23, 2015 <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>, residents in the Ivano-Frankivsk region of Western Ukraine were wrapping up their workdays and getting ready to head out into the frigid winter streets on their way to the warmth of their homes. But on this day, as one worker at the Prykarpattyaoblenergo control center was organizing his papers, he suddenly noticed that the cursor on his computer started moving quickly across the screen, completely on its own, manipulating the circuit breakers at a power substation in the region.

As he tried desperately to regain control of his computer, he was suddenly logged out. The attackers had changed his password, preventing him from logging in again.

The attackers didn't stop there. At the same time, they struck two other power distribution centers, leaving more than 230,000 Ukrainians in the dark. They had not been ready for a cyberattack of this magnitude.

But in the days, months, and years that followed, Ukraine took concrete steps to build resilience into the fabric of the country. In 2016, Ukraine launched their National Cyber Strategy, <https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/> and Ukrainian cybersecurity organizations continuously evolved to defend themselves from Russian campaigns. <https://www.cfr.org/blog/ukrainian-cyber-war-confirms-lesson-cyber-power-requires-soft-power>

Fast forward to 2022 and Ukraine would not be unprepared again. Prior to the expected Russian invasion, the private sector in Ukraine joined together with the government, as well international allies, to be ready.

Groups like the Cyber Defense Assistance Consortium <https://www.crdfglobal.org/news/crdf-global-becomes-platform-for-cyber-defense-assistance-collaborative-cdac-for-ukraine-receives-grant-from-craig-newmark-philanthropies/> brought companies together "to help Ukraine cyber defenders secure networks, hunt for and expel malicious cyber intruders, improve attack surface monitoring, and provide cyber threat intelligence to protect critical infrastructure." <https://www.crdfglobal.org/news/crdf-global-becomes-platform-for-cyber-defense-assistance-collaborative-cdac-for-ukraine-receives-grant-from-craig-newmark-philanthropies/>

This is resilience: Doing the work up front to prepare for a disruption, anticipating that it will in fact happen, and exercising not just for response but with a deliberate focus on continuity and recovery, improving the ability to operate in a degraded state and significantly reducing downtime when an incident occurs.

The courage and tenacity of the Ukrainian people in the years since 2015 and today exemplify what resilience looks like in practice, bravely demonstrating resilience every day.

The United States must follow suit and take a page out of Ukraine's cyber playbook and build its resiliency now. This goes beyond cyber resilience and the capability to swiftly recover from an extensive barrage of cyber-attacks. It also involves strengthening fundamental operational resilience to withstand both cyber assaults and other forms of aggressive physical attacks. Ukraine has demonstrated an impressive ability to quickly respond to, and effectively restore its critical infrastructure, despite facing barbaric kinetic attacks. It is critical for the United States to take inspiration from Ukraine's successes and proactively fortify its defenses and improve its response and recovery mechanisms.

This will require a major shift in approach, with a deliberate focus on three key elements: risk assessment, resilience planning, and continuous improvement and adaption.

First, organizations must identify their most critical functions and assets, define dependencies that enable the continuity of these functions, and consider the full range of threats that could undermine functional continuity.

Second, organizations must perform dedicated resilience planning, determining the maximum downtime acceptable for customers, developing recovery plans to regain functional capabilities within the maximum downtime, and testing those plans under real-life conditions.

Finally, organizations must be prepared to regularly adapt to changing conditions and threats. This starts with fostering a culture of continuous improvement, based on lessons learned and evolving cross-sector risks.

The world has watched the incredible unity of the Ukrainian people to fight on, towards victory, in the face of enormous adversity. It is our hope that in 5 years, global citizens will be able to look back and see the way our nations, our companies, and our people have worked together to learn from each other and improved our collective ability to respond to, recover, and learn from the full range of threats to our nations. We must prepare now for future attacks that we know may be coming.

The question is: Will we be ready?

CISA and Ukraine have already been strong partners in creating a culture of cyber and societal resilience. *<https://youtu.be/katci0nhcfy>* Let’s build on this work together today to create a more resilient future tomorrow.