Ranking Member John Katko

RANSOMWARE PANDEMIC
NEXT STEPS TO BOUNCE BACK

FLIP THE PARADIGM ON RANSOM PAYMENT

- Paying a ransom must be the rarest of exceptions, reserved only for the most critical or life threatening situations.

HOLD BAD ACTORS ACCOUNTABLE

- We're facing a moment of reckoning when it comes to deterrence. Adversaries like Russia are at best creating safe havens for bad actors and at worst actively creating the environment for them to operate. We must project strength.

RESOURCE CISA

- Properly resource the Cybersecurity & Infrastructure Security Agency (CISA) with the tools it needs to help the critical infrastructure community, state and local governments, and other stakeholders.
- CISA should be on a track to becoming a $5 billion agency within five years with increased capacity for its threat hunting and voluntary cybersecurity assessment services.

IDENTIFY SYSTEMICALLY IMPORTANT CRITICAL INFRASTRUCTURE (SICI)

- We need a transparent, well-understood, and stakeholder-involved process for identifying SICI, and I believe CISA is well positioned to lead on this.
- These are entities that naturally demand a deeper level of cybersecurity risk management integration with the federal government.
- I am close to revealing a legislative proposal to address this issue.
- The President must move swiftly to develop a plan to ensure continuity of the economy during a significant attack (as required by Fiscal Year 2021 National Defense Authorization Act).

INVEST ON THE FRONT END

- Companies must be constantly assessing risk and hardening systems.
- Too often we hear about systems being hardened *after* a devastating incident. While we shouldn't reflexively blame the victim, surely we can all do better.

C-SUITE AWARENESS: DEMAND BEST PRACTICES, STOP UNFORCED ERRORS

- Executives at every company should consider themselves to be cybersecurity leaders, even if they don't possess a technical background. A culture of security must start at the top. Cyber Essentials should represent the bare minimum.
- There should be no tolerance for use of unsupported (or end-of-life) software or poor password management.
- Eliminating bad practices is an easy, and necessary, first step towards more resilient digital infrastructure.

PUSH FOR CRYPTOCURRENCY TRANSPARENCY

- Disrupting the business model is one of the keys to eradicating ransomware.
- This involves following the money trail if an organization does pay the ransom. This is what I did as a prosecutor. It can be difficult, but the very nature of blockchain technology means that most transactions have a publicly visible record. We need to improve our ability to connect cryptocurrency transactions believed to be malicious to the discrete actor(s) behind them.