Evolving Cybersecurity Risks in the COVID-19 Pandemic Environment

Diana L. Burley, Ph.D.

The George Washington University

(Effective July 15th)

Vice Provost for Research

American University

“This pandemic brings out the best but unfortunately also the worst in humanity. With a huge number of people teleworking from home, often with outdated security systems, cybercriminals prey on the opportunity to take advantage of this surreal situation and focus even more on cybercriminal activities."

– Catherine de Bolle, Executive Director, Europol

Heightened Cyber Risk

- Public concern and confusion leads to opportunities for cyber criminals to exploit the collective fear and uncertainty
- Dependency on digital infrastructure
  - Increases exposure
  - Reveals uneven capabilities
  - Raises the cost of failure
- Insider threats, triggered by job insecurity and remote work may lead to the exodus of corporate and/or private data
- Awareness – Threats and behavioral drivers are not well understood; particularly outside of the workplace

Diversified Attack Vectors

- Spam emails with phishing campaigns
- Ransomware attacks targeted at medical facilities, research centers
- Malicious domains with names that suggest legitimate content regarding the pandemic
- Malware, spyware
- Disinformation and misinformation campaigns

Prime Targets

- Traditional targets (business, individuals)
- COVID-19-related research
- US Pandemic response
- Supply chains

Cybercriminals adapted quickly to capitalize on the pandemic

- US cybercrime reports quadrupled *(FBI)*
- Cybercrime, more than other criminal activities, has been the most visible in the pandemic environment *(Europol)*
- Motives include both profit and geopolitical interests

Discussing the evolving cybersecurity threats and risks to government, universities, and industry

Expert Panelists

Brandon Wales, Department of Homeland Security

Brian Abrahamson, Pacific Northwest National Laboratory