REQUEST FOR COMMENT RESPONSE

School and Libraries Cybersecurity Pilot Program

WC Docket No. 23-234

December 12, 2023

I. INTRODUCTION

In response to the Federal Communications Commission's ("FCC") notice of proposed rulemaking ("NPR") to create the Schools and Libraries Cybersecurity Pilot Program ("pilot program"), CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

We appreciate the FCC's efforts to better protect the sensitive data from K-12 schools and libraries, and to ensure that students pursue education without disruption from cyber attacks. Cybersecurity threats are evolving and increasing across all sectors, and the education sector is among the more heavily-targeted. Illustrative of this, in CrowdStrike's 2023 *Global Threat Report*, we observed a 50% increase in the number of interactive intrusion campaigns and a 112% increase in access brokers selling their services (from 2021 - 2022), both of which frequently affect educational institutions and other public sector entities.[1]

Malicious actors are opportunistic and in many instances do not discriminate in their targeting. In fact, we saw the largest increase in access brokers targeting academic institutions from 2021 - 2022 across all sectors. Additionally, ransomware continues to

[1] 2023 *Global Threat Report*, CrowdStrike, https://www.crowdstrike.com/global-threat-report/

be one of the most common types of attacks affecting schools, and those campaigns seek to leverage the coercive effects of school disruptions.

As the NPR notes, almost all forms of K-12 education have some type of online component and school networks include a variety of devices and endpoints. The E-Rate program has successfully given many schools the funds to procure the technologies needed to make use of new ways of learning. However, as we noted in previous comments to the FCC regarding the public notice on *Requests to Allow the Use of E-Rate Funds for Advanced or Next-Generation Firewalls and Other Security Services*,[2] CrowdStrike supports the expansion of funding to include cybersecurity security tools to protect K-12 schools and libraries from cyberattacks.

With this in mind, CrowdStrike supports the FCC's initiative to create the pilot program. We believe this pilot program and funding will have a positive and near-term impact to better protect K-12 schools, libraries, and the teachers and students. We also appreciate the numerous government guidelines, government programs, and industry programs (including CrowdStrike's Falcon Go[3]) that are referenced throughout the NPR. The FCC correctly notes that there are many already existing guidelines, such as the Cybersecurity and Infrastructure Security Agency's "*Protecting Our Future: Partnering to Safeguard K-12 organizations from Cybersecurity Threats*" report and its complementary online toolkit, that K-12 schools and libraries can reference as they are building their cybersecurity programs. Additionally, there are programs from government or industry that entities can leverage to create an affordable security plan.

While we do not have feedback on every question in the public notice, we do want to offer responses to several questions along with overarching comments that may be of value to the FCC as it builds the pilot program.

A. *Question*: What security measures, including equipment and services, should be made eligible to participate in the Pilot?

---

[2] CrowdStrike comments to FCC on *Requests To Allow the Use of E-Rate Funds for Advanced or Next-Generation Firewalls and Other Network Security Services*, https://www.crowdstrike.com/wp-content/uploads/2023/04/FCC-E-Rate-Comments.pdf

[3] CrowdStrike Falcon Go, https://go.crowdstrike.com/try-falcon-pro-cybersecurity-overview.html?utm_campaign=falcontrial&utm_content=ecom-treq-en-fpro-tct-us-psp-smb-trl-cybr-x_x_x_x-x&utm_medium=sem&utm_source=goog&utm_term=cybersecurity%20software&gad=1&gclid=EAIaIQobChMI9s2O5-mO_wIVqvfjBx0f5Q23EAAYASAAEgLJr_D_BwE

CrowdStrike recommends that the FCC include tools that are not overly prescriptive so that schools can choose the best security practices for their level of risk. Organizations should leverage several key technologies to defend against cyber threat actors:

- **Cloud Services**. Leveraging cloud systems provides a series of potential security enhancements. Retiring legacy applications and infrastructure reduces attack surface and points of failure. Cloud systems enable comprehensive visibility of workloads. For security technologies specifically, native cloud-based solutions provide robust and scalable protection of distributed environments.

- **Endpoint Detection and Response (EDR)**. EDR is the cybersecurity approach to defending endpoints such as desktops, laptops, and mobile devices from malicious activity. Given that schools have so many connected devices, EDR would be helpful in identifying and preventing threats and enabling threat hunting activities in case adversaries gain unauthorized access.[4]

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats based on behavior cues rather than known signatures. Machine learning and artificial intelligence are essential to this end. Leveraging these technologies is essential to meeting constantly-evolving threats.

- **Identity Protection and Authentication**: As schools embark on a digital transformation to remote learning, Bring-Your-Own-Device policies become commonplace, cloud services multiply, and enterprise boundaries continue to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly determine and respond to identity-based attacks.

Additionally, there are multiple security program requirements that bolster organizations' security posture:

[4] The next evolution of the EDR concept, Extended Detection and Response (XDR), seeks to leverage rich endpoint telemetry and other security-relevant data, wherever it exists within the enterprise. EDR is a natural baseline security capability, but XDR drives more comprehensive cybersecurity outcomes.

- **Speed**. When responding to a security incident or event, every second counts. The more defenders can do to detect adversaries at the outset of an attack, the better the chances of preventing them from achieving their objectives. Adversaries work rapidly at the outset of breach to move laterally and escalate privileges, seeking to gain access to more systems and data and ensure persistence. This means that organizations should measure and reduce their response time.[5]

- **Threat Hunting**. Whether through supply chain attacks or otherwise, adversaries periodically breach even very-well defended enterprises. However, properly trained and resourced defenders can find them and thwart their goals. Proactive hunting is a leading indicator of the strength of an enterprise cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. The better-instrumented the environment, the more chances defenders give themselves to identify malicious activity as an attack progresses through phases. Multiple opportunities for detection increase defenders' chances of success and help avert "silent failures."

- **Zero Trust Architecture.** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust architecture concepts radically reduce or prevent lateral movement and privilege escalation during a compromise.

- **Logging Practices**. Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

- **Managed Service Providers**: Some entities lack the cybersecurity maturity, or workforce, to run robust security programs internally. Increasingly, such entities should rely upon managed security service providers to strengthen their security posture. K-12 schools and libraries should consider leveraging a managed security services provider, because it allows them to have 24/7 coverage 365 days a year to detect and respond to threats. While these types of

[5] Elite organizations seek to identify a breach attempt within one minute, investigate within ten minutes, and isolate or remediate threats within sixty minutes.

services may cost more than standard tools alone, they are less expensive than building an entire security operation from scratch or dealing with a breach.

These technologies and security program requirements should be included in the pilot program. Additionally, many of these listed items may include on-going, recurring costs. The pilot program should support on-going costs in addition to one-time purchases.

B. *Question*: Should Pilot participants be required to submit data on the number of intrusion attempts, number of successful attacks, mean time to detection and response, estimated cost of each attack, etc.?

We recognize that gathering data to tell a story about the success or failure of a pilot program is an important part of the process; however, data such as the number of intrusion attempts and estimated cost of each attack is subjective and difficult to measure. Mean time to detection and response, however, is a promising metric, and we recommend utilizing it to measure performance where possible.[6] This would be most straightforward by leveraging performance indicators from a trusted Managed Security Services Provider.

Further, it is unlikely that many K-12 schools and libraries were measuring this information before the beginning of the pilot program. This means the FCC may encounter difficulties measuring performance improvements *within* pilot participants. The most straightforward solution here would be to designate a 'control group' of similar organizations to measure after a notional pilot performance period, and to subject them to a thorough, professional Compromise Assessment at the end of the pilot window.

C. *Question*: The NPR asks about the budget and length of the pilot program. Additionally, it asks how programs should be funded following the completion of the pilot program.

The pilot program will have a $200 million budget over a three year period. While this is a substantial investment from the FCC, with there being over 100,000 K-12 schools in

[6] CrowdStrike refers to the 1-10-60 rule — detecting an intrusion within 1 minute, investigating within 10 minutes and isolating or remediating the problem within 60 minutes – as a goal for organizations to adhere to. The longer an adversary is allowed to engage in lateral movement over a protracted dwell time, the more likely an attack will eventually succeed.

the U.S., there could potentially be more applications for the pilot program than funding can support.

We recommend that at least 18 months before the end of the pilot program, the FCC releases a public notice outlining their plan for sustaining cybersecurity services for K-12 schools and libraries on a more permanent basis, so that entities can adjust their budgets accordingly. The NPR notes E-Rate or the Universal Service Fund are potential methods for funding after the pilot program.

III. CONCLUSION

The FCC's NPR provides a thoughtful analysis of a complex, constantly evolving, policy area and an innovative solution to solve the problem. As the pilot program moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend that the pilot program focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike®, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Manager, Public Policy

Email: policy@crowdstrike.com

***