HOW TO BOOST YOUR ORGANIZATION'S CYBERSECURITY, INCLUDING GETTING GRANT FUNDING

Hackers have long targeted public safety organizations and local governments, and the threat of cyberattacks is real and growing. Cybersecurity requires a significant investment, but it's imperative that public safety agencies take measures to protect critical infrastructure from ransomware and other attacks.

Here are 10 strategies your organization's cybersecurity plan should include to help prevent data breaches and system compromises, plus links to grants resources to help you fund those efforts.

10 CRITICAL CYBERSECURITY MEASURES

1. Mandate the use of multi-factor authentication to make it harder to break into your system.
2. Change passwords across your networks to make previously stolen credentials useless.
3. Educate employees about common tactics that attackers use and encourage them to report anything suspicious.
4. Ensure that all software is up to date so that systems are patched and protected against known vulnerabilities.
5. Confirm that your organization's entire network is protected by antivirus/antimalware software that continuously hunts and mitigates threats.
6. Disable all ports and protocols that are not essential for business purposes.
7. Back up your organization's data, maintain secure offline backups and encrypt the data so it is useless if stolen.
8. Designate a crisis response team for suspected cybersecurity incidents and identify roles/responsibilities within the organization, including technology, communications, legal and business continuity functions.
9. Conduct exercises of your emergency plans to ensure that all participants are prepared to respond quickly to minimize the impact of an attack.
10. The Cybersecurity and Infrastructure Security Agency leads the national effort to understand, manage and reduce risk to cyber infrastructure. Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats. Report anomalous cyber activity and cyber incidents 24/7 to report@cisa.gov or 888-282-0870.

GAIN PEACE OF MIND WITH A TRUSTED PARTNER

Thwarting cyberattacks is a huge and ongoing undertaking that may be beyond the financial and technical capabilities of many public organizations. Partnering with a managed security service provider like Motorola Solutions to provide 24/7 cybersecurity monitoring, detection and response may be a more effective strategy than maintaining your own 24/7 security team in-house.

GET GRANTS TO FUND YOUR CYBERSECURITY EFFORTS

Cybersecurity doesn't come cheap, but the alternative is far more costly. The good news is that a new federal program of grant funding is available for cybersecurity efforts:

Department of Homeland Security State and Local Cybersecurity Grant Program

- $1 billion available federal funds to state, local and tribal governments to address cybersecurity risks and threats.
- Requires states to develop comprehensive cybersecurity plans describing steps to be taken to implement continuous cybersecurity vulnerability assessments and threat mitigation.
- Applications are expected to open during the third quarter of 2022. Watch DHS.gov or Grants.gov for details and application information.

Applying for grants can be challenging. To help, Motorola Solutions offers assistance and has partnered with Lexipol's grant experts to offer a wide range of free grants help programs, which include:

- Free customized grant research specific to department needs.
- Grant alerts for upcoming grants.
- Unlimited free grant consulting from senior grant consultants.
- Discounted grant writing services.

EducationGrantsHelp GovGrantsHelp

MOTOROLA SOLUTIONS