Accession Number:	H0571	**ECRI Priority:**	High	**Published:**	03/20/2020
Channel:	Devices	**FDA:**	Not Specified	**Last Updated:**	03/20/2020

[COVID-19] Expanded Work from Home Policies May Pose Increased Security Risks [ECRI Exclusive Hazard Report]

Problem

The increased amount of employees working from home during the COVID-19 health emergency poses security risks.

ECRI Recommendations:

1. Evaluate the remote access and VPN configuration for increased volume and new use cases.
    - Split-tunnel configurations may increase risk by allowing traffic to bypass perimeter security controls (e.g., firewalls, web filters, data loss prevention [DLP]).
    - Refer to ECRI's 2018 Top 10 Hazard regarding remote access, Hazard H0471.
    - Follow best practices when possible (see the NIST solutions here).
    - Exercise caution while applying changes to configurations.
2. Ensure that Endpoint protection or antimalware systems are remotely updatable and configurable.
3. Evaluate remote access and VPN usage policies and modify for the current COVID-19 health emergency.
4. Educate employees on the following:
    - Proper use of work from home resources including remote access systems or VPNs.
    - HIPAA policies and handling of PHI.
    - Phishing awareness (see Hazard H0570).

Background:

1. Healthcare providers are enforcing work from home policies during the COVID-19 health emergency. This poses increased security risks.
2. Employees inexperienced with working from home may need to be educated on practices including:
    1. Acceptable use of work devices at home.
    2. The handling of PHI at home.
3. Remote access systems, VPNs, and security controls may not be configured to:
    - Handle increased load.
    - Support workflow from new types users who are now teleworking.
    - Allow essential system updates from remote devices.
4. To accommodate increased traffic on VPNs, some facilities may choose to allow some traffic to bypass perimeter controls (split-tunneling). While this may be necessary, it inherently increases risk.

References:

- ECRI. Hackers can exploit remote access to systems, disrupting healthcare operations [top 10 hazards list online]. 2018 Nov 1 [cited 2020 Mar 20]. Available from Internet: Click here.
- National Institute of Standards and Technology. Security for enterprise telework, remote access, and bring your own device (BYOD) solutions [online]. 2020 Mar [cited 2020 Mar 20]. Available from Internet: Click here.

Geographic Region(s)

Worldwide

Suggested Distribution

Clinical/Biomedical Engineering, Risk Management/Continuous Quality Improvement, Information Technology

Comment

• This alert is a living document and may be updated when ECRI receives additional information.