Dear Merit Members,

I'd like to take a moment to address recent international cyber threats and provide some best practices to keep your organizations secure.

Over the last few weeks, hackers originating from Russia have coordinated attacks against individuals, governments, corporations and Internet Service Providers. These attacks are currently being directed toward IoT devices, home based modems and corporate routers, switches and firewalls. These nefarious activities are an attempt at an organized attack against the US and UK, with the goal of bringing down critical infrastructure. What may have started these attacks could be directly tied to Russian diplomats being expelled from a number of countries. In addition, an attack was launched against Russian network equipment with the message, "Stop messing with our elections," being left behind. (Read more about this at https://www.cyberscoop.com/russian-hackers-routers-united-states-britain/) There are simple changes that you can make to your company infrastructure, even your home equipment, to safeguard assets that you own.

1. Change default settings - The default username and password on all equipment is insecure. Theses credentials provides administrative access to equipment and can easily be found online. Changing the default password on all equipment should be the very first thing you do.
2. Maintain system level updates - Ensure that you are patching your network equipment at least quarterly.
3. Place access lists on management interfaces - This restricts equipment login access geographically. Firewall rules can be configured to only allow authentication attempts from known trusted networks.
4. Replace end of life/end of support equipment - High end network equipment can cost hundreds of thousands of dollars. Ensure that your organization is budgeting for replacement of aging devices so that you can continue to apply patches to your network and security equipment. An

information breach or complete network outage could potentially cost your organization more than the purchase of newer equipment.

These are a handful of “quick wins” to better protect your network equipment from attack, whereas others may take a while to implement due to budget constraints. If your organization requires additional security, but lacks the budget to support high-level cybersecurity personnel, Merit Community CISO can help.

Merit Community CISO services will assess your attack surface, identify weaknesses, develop security strategies that significantly minimize your chance of a data breach and provide guidance on regulatory compliance and reporting, all without the expense of hiring a full-time Security Officer.

For more information, visit merit.edu/CISO.

Merit also offers a community of practice for security professionals to share best practices and network with their peers (SCOPE).

For information on our next meeting, visit merit.edu/scope.

Thank you,

Jason Brown, CISSP
Chief Information Security Officer
jbrown@merit.edu | 734.527.7210 p | 734.527.5790 f | www.merit.edu