By Stacey Wright[i] and Michael Yu[ii]

We know. We get it. Training that even hints of being related to “cyber” don’t sound fun or productive. Despite that, we all know that almost everything is cyber-related, from emails, to digital forensics on smartphones and tablets. And all of that opens new potential vulnerabilities.

Business Email Compromise

One of the most common scams right now is the Business Email Compromise (BEC), which is responsible for $5.3 billion dollars in losses since October 2013. In its most basic format, a malicious actor emails the finance staff pretending to be the department’s executive or director. The subsequent email exchange results in the finance department sending a wire transfer to the malicious actor’s account.

Ransomware

On a different front, one of the most talked about types of malware is ransomware. While almost all ransomware is opportunistic, meaning it targets victims indiscriminately, law enforcement agencies have also been infected. In both these instances, following a couple of cybersecurity best practices can prevent your entire network from becoming encrypted.

Implementation

So how can you implement a cybersecurity awareness program that isn’t too painful? The first step is to identify what you have in place so you know where your gaps are. The National Institute of Standards and Technology (NIST) has created a Cybersecurity Framework that provides industry standards and best practices for managing cybersecurity risks in a cost-effective way. Taking this one step further, the U.S. Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are running the National Cyber Security Review from October 2nd through December 15th. This is a free, anonymous, annual self-assessment, based on the NIST Cybersecurity Framework, which provides survey takers with a metric-based report containing recommendations for improvement, and year-to-year comparisons to document maturity growth.

Once you have a baseline, you can identify where to go from there. The NIST Cybersecurity Framework defines maturity models (section 2.2.) that can help. The SANS Institute, one of the best cybersecurity training agencies out there, has also put together a Security Awareness Roadmap with concrete steps to follow in order to improve your cybersecurity posture.

Regardless of which you choose, there are some additional, basic cybersecurity hygiene steps you can take to ensure your department is becoming safer.

Cybersecurity Hygiene Steps

1. **Designate** someone to be the cybersecurity expert and then make sure they get some extra training and have the resources to implement changes in the department.
2. Have **your own web domain and official email addresses**. Whether you share this with your town/county or have a police department specific domain, it's important your officers have official email addresses acceptable for sending and receiving secure communications.
3. **Patch!** Over time software and hardware systems become vulnerable and vendors issue patches to fix the vulnerabilities. Having a patch management program that keeps your software and hardware up-to-date is one of the best things you can do to secure your network.
4. Use **antivirus software**, and just like the other software, keep it up-to-date!
5. **Back it up!** Backing up all your critical files is the best way to mitigate the effects of ransomware and many other types of malware infections. Ask your cybersecurity expert to work with your Information Technology department to make sure critical files are saved to a second, offline location at least once a day. And then test to make sure you can restore them!
6. **Enforce strong, unique passwords**. Every day we come across leaked lists of user names and passwords. If you reuse passwords in different locations and one of those locations is compromised, it's trivial to identify your department and try to login into your network with the leaked information. Yes, that means that the lack of cybersecurity in your bowling league can put your department at risk!
7. **Share!** It's always hard to go alone, so work with others. Join communities of experts, like the USSS Electronic Crime Task Force, FBI's Cyber Task Force and InfraGard, the MS-ISAC, and use the resources on the Police Executive Research Forum and International Associations of Chiefs of Police Law Enforcement Cyber Center.
8. And finally, **educate all your employees**. The free cybersecurity courses available to law enforcement officers through the National White Collar Crime Center are great for educating officers who work cyber matters and the chain of command. But all employees should understand why unique passwords, safe Internet browsing, intelligent social media use, mobile device security, and careful cloud storage are important. This enables the people within a department to be part of the solution.

   There are lots of basic courses out there. One, recommended by many state and local governments, is the SANS Securing the Human program. The Center for Internet Security's (CIS) CyberMarket is a trusted, collaborative purchasing program for U.S. state, local, tribal, and territorial governments. Twice a year CyberMarket offers large discounts on SANS training, including Securing the Human, so you can even get this training at a huge discount. The next buy window is January and February 2018, which makes this the perfect time to find the funding to train all of your employees.

There. Now you've got the beginnings of a plan that you can start today. And while this won't protect against every threat, following these steps will help you build a cybersecurity awareness program and protect your department.

Now, that wasn't too bad, was it?

Photo Credits: "202598437 Copyright Your_photo. 2017 Used under license from Bigstockphoto.com"; "165755138 Copyright ValeryBrozhinsky. 2017 Used under license from Bigstockphoto.com"; "70728256 Copyright Pressmaster. 2017 Used under license from Shutterstock.com"

[i] Stacey A. Wright is the Senior Intel Program Manager at the Center for Internet Security (CIS), where she runs the Intel Team for the Multi-State Information Sharing and Analysis Center (MS-ISAC). She co-developed the MS-ISAC Intel Team to focus on providing strategic and operational cyber threat intelligence to state, local, tribal, and territorial (SLTT) governments. The products provide SLTT government-focused insight on risks, actors, trends, vulnerabilities, and incident response, allowing CISOs to improve visibility, detection, accuracy, and strategically align resources to the current cyber environment. In addition to her work at CIS, Stacey teaches two graduate cybersecurity and threat intelligence classes at the State University of New York, College of Emergency Preparedness, Homeland Security, and Cyber Security. Prior to CIS, Stacey was the Cyber Intelligence Analyst for the Federal Bureau of Investigation (FBI) Albany Division, where she was responsible for coordinating the local cyber intelligence program and served as the FBI's liaison to the MS-ISAC. Stacey began her career as an Information Systems Specialist for the Cambridge, MA, Emergency Communications and Fire Departments. She received her Bachelor of Science in Criminal Justice from Northeastern University, and her Master of Business Administration from the University of Massachusetts, Boston.

[ii] Michael Yu is a Sergeant with the Montgomery County Department of Police with fifteen years of law enforcement experience. He has been a digital forensic examiner for approximately seven years. Sergeant Yu has worked assignments in uniformed patrol, Alcohol Enforcement Unit, Firearms Task Force, District Investigative Bureau, Electronic Crimes Unit and Hostage Negotiator Team. He has testified as a digital forensics expert in local, state and federal courts and holds a B.A. degree in Criminal Justice and Criminology from the University of Maryland, College Park.