



## **TLP White**

### ***Policy Analysis – EXERCISE EXERCISE EXERCISE***

This past week, NH-ISAC announced the launch of a new tabletop exercise – *Cyber Outbreak*.

*Cyber Outbreak* will test the sector’s ability to respond to cyber-threats, share information, and maintain resilience during attacks against critical infrastructure. To do this we will hold regular tabletops over the next year that evaluate threats against different sub-sectors. The exercises will initially just include members of NH-ISAC, but will likely expand to include organizations from other interconnected sectors as well as the Government.

The first exercise in the series will be held on November 27, as the NH-ISAC Fall Summit gets underway in Scottsdale, Arizona. The scenario for the first exercise will be derived from the experiences and lessons learned during the “WannaCry” and “NotPetya” attacks. We will test information sharing capabilities between health care organizations as well as other sector-wide response capabilities.

If you’d like to participate in the kick-off exercise, please register [here](#).

### ***Hot Links –***

The Office of the National Coordinator for Health Information Technology at HHS [dropped](#) some big news last week, loosening testing and certification requirements.

First, they reduced the requirements on third party testing – organizations will now be able to “self-declare” certification on 30 of 55 certifications that are required. Second, ONC indicated they would not enforce the requirement for third party testing companies to conduct randomized surveillance on certified health IT products and services.

Having a list of government approved certification companies may not have been the most efficient way to tackle security auditing, but it’s not like the sector has [proved so adept](#) at defending itself. The test of whether this approach works will be if and how enforcement actions take place when a self-declaring certification is exploited.

--[HHS Continues its work on Cybersecurity Guidance](#) (HIMSS)

--[Apple, Fitbit Chosen for FDA Pilot to Accelerate Digital Health Tech Approval](#) (healthcare informatics)

September 28, 2017

- [Broadening HSTS to secure more of the Web](#) (Google)
- [Goodbye, login. Hello, heart scan.](#) (U Buffalo)
- [Unmetered Mitigation: DDoS Protection Without Limits](#) (CloudFlare)

### ***The Week Ahead –***

#### ***Congress –***

- Tuesday, Oct. 3: Oversight of the Equifax Data Breach: Answers for Consumers ([House Commerce](#))
- Wednesday, Oct. 4: Hearings to examine the Equifax cybersecurity breach ([Senate Banking](#)) (Senate Judiciary – [Subcommittee on Privacy, Technology and the Law](#))

--Facebook, Twitter, and Alphabet have been invited to an open hearing on Russia meddling in the 2016 election in front of Senate Intel on November 1 ([Chicago Tribune](#))

#### ***Conferences and Webinars –***

- [Business E-mail Compromise \(BEC\) Workshop](#) – San Francisco (NH-ISAC) (10/13)
- [Business E-mail Compromise \(BEC\) Workshop](#) – Seattle (NH-ISAC) (10/16)
- [Health IT Summit – Raleigh](#) (NH-ISAC) (10/19)
- [Business E-mail Compromise \(BEC\) Workshop](#) – Kennedy Space Center (NH-ISAC) (10/19)
- [Business E-mail Compromise \(BEC\) Workshop](#) – Akron (NH-ISAC) (10/25)
- [Business E-mail Compromise \(BEC\) Workshop](#) – Phoenix (NH-ISAC) (10/26)
- [Business E-mail Compromise \(BEC\) Workshop](#) – Denver (NH-ISAC) (10/27)
- [Business E-mail Compromise \(BEC\) Workshop](#) – Nashville (NH-ISAC) (10/30)
- [Biotec/Pharma Security Workshop at MSD, Prague](#) (NH-ISAC) (11/7)
- [Health IT Summit – LA](#) (NH-ISAC) (11/9)
- [Cyber Outbreak](#) (NH-ISAC) (11/27)
- [NH-ISAC Fall Summit – Cyber Rodeo](#) (11/28-30)
- [Health IT Summit – Dallas](#) (NH-ISAC) (12/14)

#### ***Reports –***

- [Protenus breach report](#) (via [healthcare informatics](#))
- [Europol Internet Organised Crime Threat Assessment 2017](#)

#### ***Podcasts –***

- [Keyboard warrior: the British hacker fighting for his life](#) (Guardian)
- [Aetna's new approach to authentication w/ Jim Routh!](#)

#### ***Breaches –***

- [Equifax directed consumers to fake phishing site for weeks](#) (HelpNet)
- [Sonic](#) (info security)
- [Deloitte](#) (Krebs)

#### ***Sundries –***

##### ***Policy:***

- [Shrinking Anonymity in Chinese Cyberspace](#) (Lawfare)

September 28, 2017

- DHS Secretary (Acting) Testifies before Congress – [written testimony](#) (DHS)
- SEC Chairman Testifies before Congress – [written testimony](#) (SEC)
- [State plans to elevate cyber mission, despite shuttering dedicated office](#) (NextGov)

**Threats:**

- [46,000 new phishing sites are created every day](#) (HelpNet)
- [WannaCry ransomware explained: What it is, how it infects, and who was responsible](#) (CSO)

**Vulnerabilities:**

- [Major security vulnerability discovered in new Mac OS](#) (NextGov)

**Network defense:**

- [Your head could roll in next cyber breach](#) (Federal News Radio)
- [DHS commercializes two nature-themed cyber products](#) (NextGov)
- [Alabama Medicaid Data Security, Information Security Can Improve](#) (HealthITSecurity)
- [Recommendations to Guide Secure Interoperability](#) (HIMSS)
- [How Health Data Security Relates to Healthcare Biometrics](#) (HealthITSecurity)
- [The Implications for HIT Leaders of Accelerating Market Consolidation? There Are Many](#) (healthcare informatics)
- [Survey: 73 Percent of Medical Professionals Share Passwords to Access EHRs](#) (healthcare informatics)
- [Nurses, Physicians Use Personal Devices Even When BYOD is Prohibited](#) (healthcare informatics)
- [Firefox takes a Quantum leap forward with new developer edition](#) (ars)

**(In)Secure Takes** – Twitter's best from the week



**SwiftOnSecurity**  
@SwiftOnSecurity



If your network gets owned the same time as everybody else through a supply chain compromise, is that a Hackt of God.

9/19/17, 7:51 PM

---

September 28, 2017



**briankrebs** ✓  
@briankrebs



Gee, Experian, what's point of a freeze if I can just submit SSN, DoB, address & get someone's PIN emailed 2 me? [experian.com/ncaonline/fre...](https://experian.com/ncaonline/fre...)

9/21/17, 9:15 AM



**SwiftOnSecurity**  
@SwiftOnSecurity



The only problem Equifax has with hackers viewing your private info is the hackers didn't pay them enough.

9/20/17, 12:15 PM


September 28, 2017



**briankrebs**   
@briankrebs



Hey @Equifax 1999 called and wants its browsers (Internet Explorer and Netscape) back.



---

## Security and Encryption

In the United States, you can order all Equifax products online with confidence using Netscape and Internet Explorer, since they support the recommended 128-bit key length encryption SSL (Secure Sockets Layer). International versions support 40-bit encryption.

### SSL and 128-bit Encryption

If you have Netscape Navigator, simply select 'Help' from the Menu Bar, then click on 'About Netscape' and you will obtain a screen of information including the version.

If you see language referring to 'International Security', then your browser does not support 128-bit encryption. If you see language referring to 'U.S. Security' or 'Domestic Security,' then your browser does support 128-bit encryption.

If you have Internet Explorer, go to a secure page (a secure page uses the prefix 'https'). With your cursor positioned anywhere on the secure page, click on File (from the main menu), then Properties. Click on the tab marked 'Security' and look under the heading 'Privacy strength.' It will show you have 128-bit or 40-bit encryption.

### To See if Your Session Is Encrypted

If you are running Netscape Navigator, look in the lower left-hand corner of the browser. You will see a small key as an indication that your session is running in an encrypted mode. When your session is not encrypted you will see a broken key. If you are using Internet Explorer, you will see a lock icon displayed in the bottom right corner of the window when you are on a secure page.

### To See if 128-bit Encryption is Enabled

If you are using Netscape Navigator, it is possible that your 128-bit encryption feature may be disabled.

To verify, select 'Options' then 'Security Preferences' then 'General.' There should be a check next to the 'Enable SSL v2.' Click on the 'Configure' button. The 'Configures Ciphers' window will appear.

Make sure the first item (RC4 encryption with a 128-bit key) is checked, then click on 'OK'. Microsoft Internet Explorer does not allow you to turn the security features off.

Contact us: follow @NHISAC and email at [bflatgard@nhisac.org](mailto:bflatgard@nhisac.org)