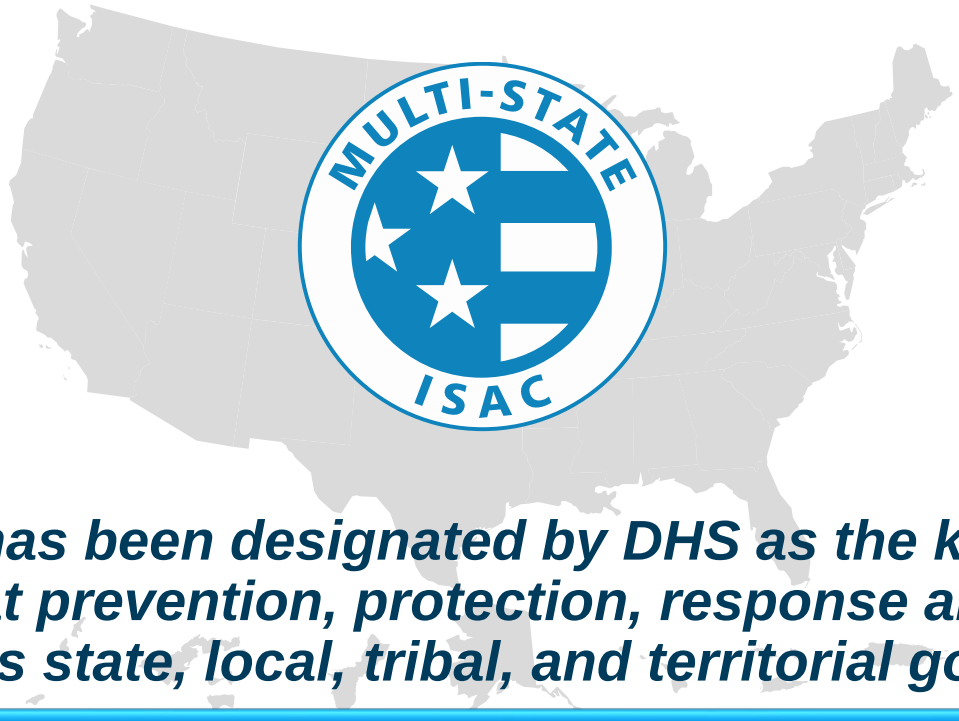
Information Sharing Resources for Municipal Utilities

Kyle Bryans

Program Specialist

MS-ISAC

Multi-State
Information Sharing and Analysis Center



The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial governments

https://www.cisecurity.org/ms-isac/

Why SLTT Governments?

Criminals look for data...
and governments have a lot of it!

Why care? - Employee Mistakes

Why care? - Employee Mistakes

Why care? – Employee Mistakes

24 x 7 Security Operations Center

Central location to report any cybersecurity incident

- **Support:**
  - Network Monitoring Services
  - Research and Analysis
- **Analysis and Monitoring:**
  - Threats
  - Vulnerabilities
  - Attacks
- **Reporting:**
  - Cyber Alerts & Advisories
  - Web Defacements
  - Account Compromises
  - Hacktivist Notifications

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Network Monitoring (Albert)

- Signatures unique to SLTT governments
- 24x7x365 research, analysis, and support
- Integration of research on specific attacks and actors, including nation-state actors (APT)
- Real-time information sharing with SLTT partners
- Experienced cybersecurity analysts who review each event minimizing the number of false-positive notifications

Albert
CIS Network Monitoring

Monitoring of IP Range & Domain Space

IP Monitoring

- IPs connecting to malicious C&Cs
- Compromised IPs
- Indicators of compromise from the MS-ISAC network monitoring (Albert)
- Notifications from Spamhaus

Domain Monitoring

- Notifications on compromised user credentials, open source and third party information
- Vulnerability Management Program (VMP)

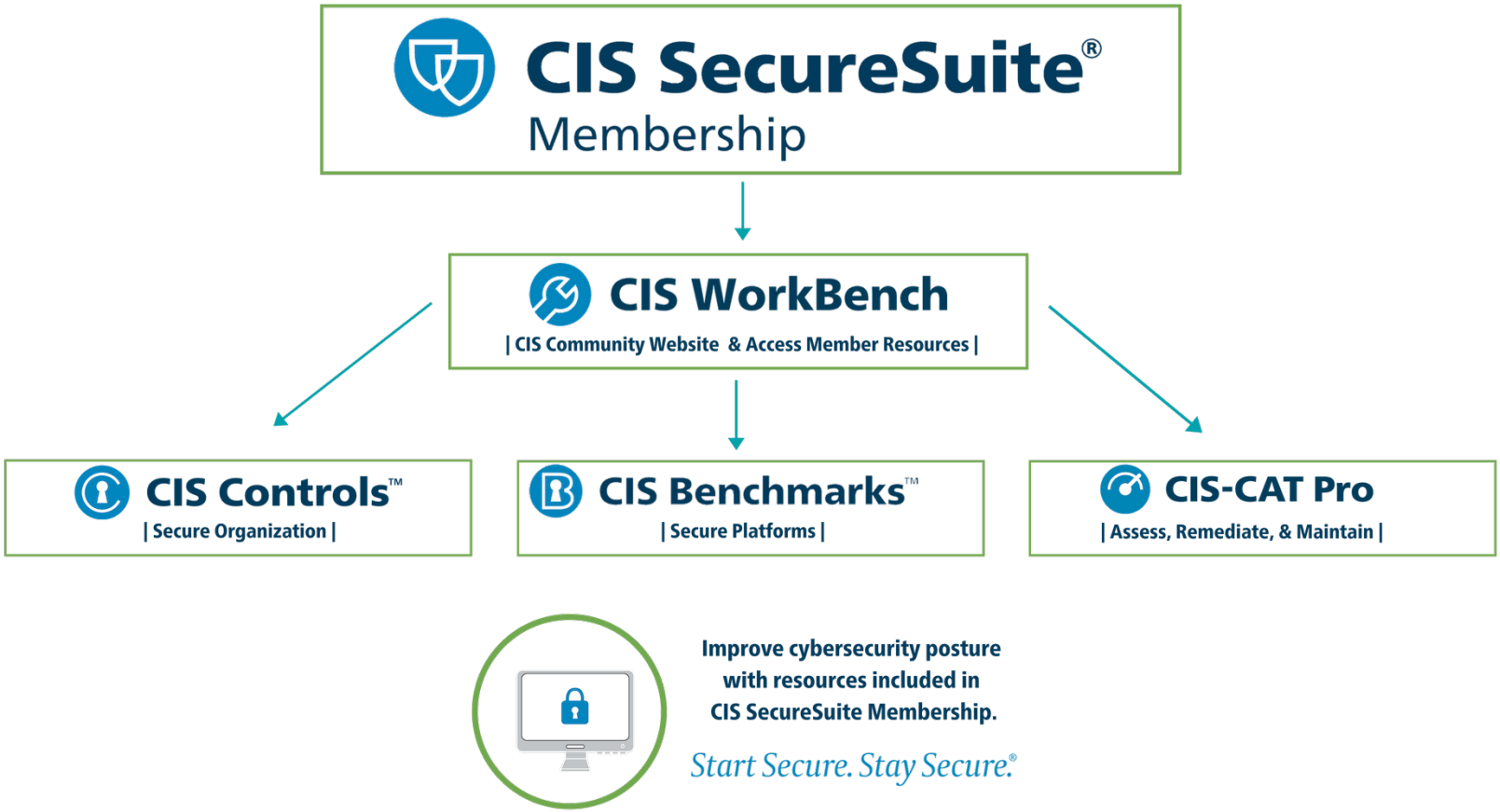
Send domains, IP ranges, and contact info to:
soc@cisecurity.org

Computer Emergency Response Team

- Incident Response (includes on-site assistance)
- Network & Web Application Vulnerability Assessments
- Malware Analysis
- Computer & Network Forensics
- Log Analysis
- Statistical Data Analysis

To report an incident or request assistance:
Phone: 1-866-787-4722
Email: soc@cisecurity.org

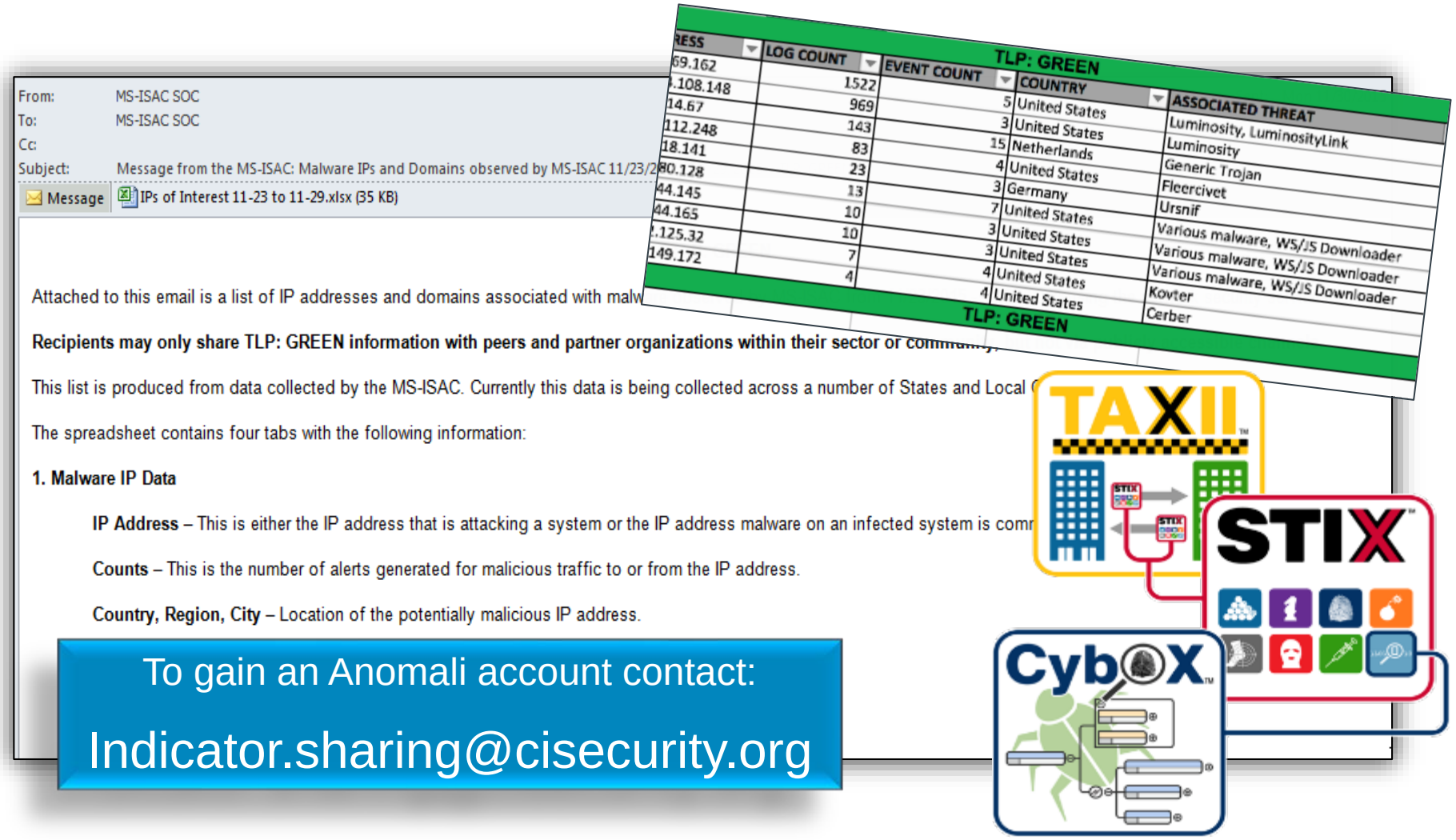
CIS SecureSuite



MS-ISAC Advisories

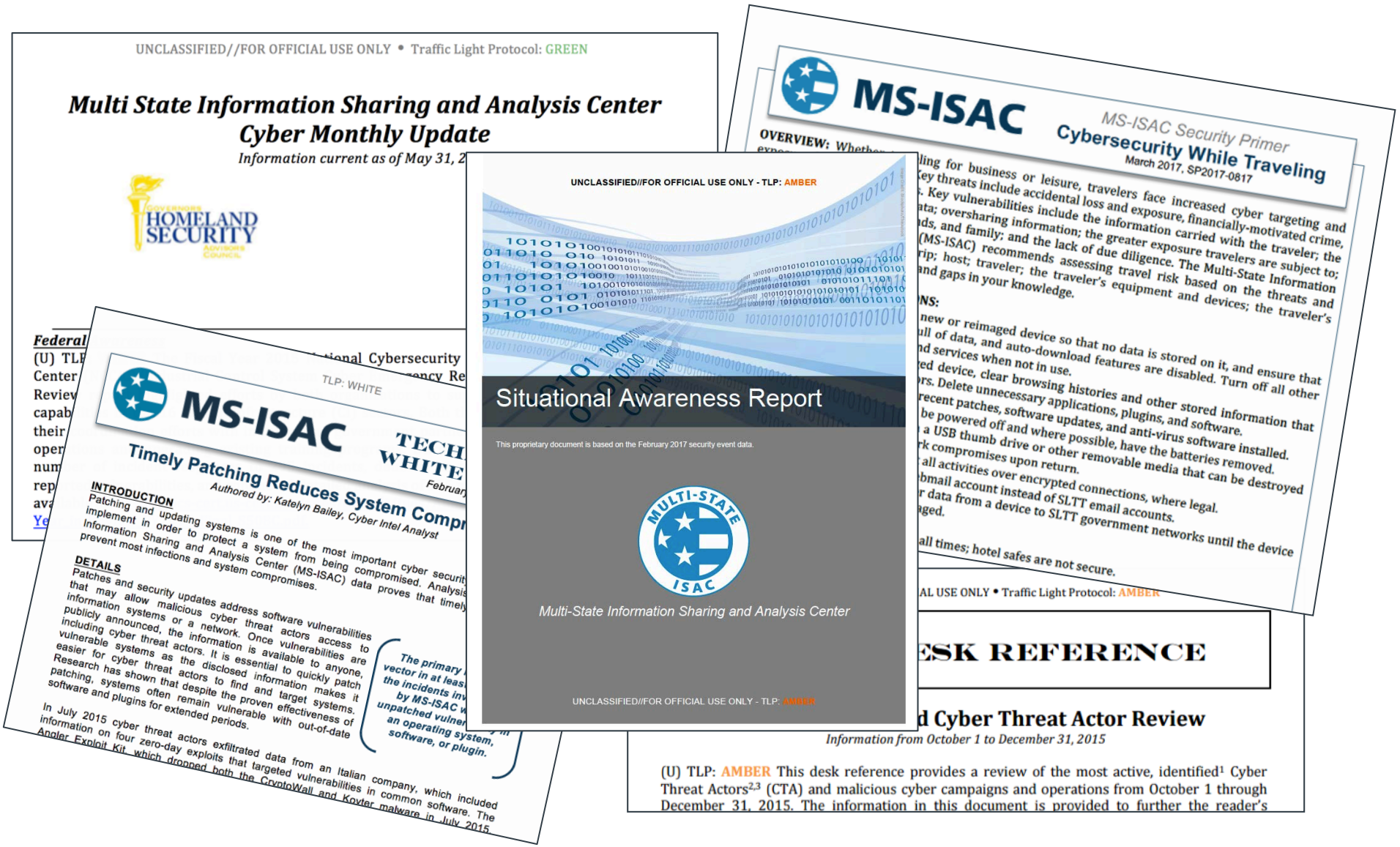
Weekly Malware IPs and Domains

Automated Threat Indicator Sharing via Anomali



TLP: WHITE

MS-ISAC Intel Papers



TLP: WHITE

MS-ISAC Cyber Alerts

MS-ISAC Advisory
Sent: Thursday, June 16, 2016 at 2:57 PM
To: Thomas Duffy

TLP: WHITE
MS-ISAC CYBER ALERT

TO: All MS-ISAC Members, Fusion Centers, and IIC partners

DATE ISSUED: June 16, 2016

SUBJECT: Malicious Email Campaign Targeting Attorneys Spoofs Emails From Statewide Legal Organizations - TLP: WHITE

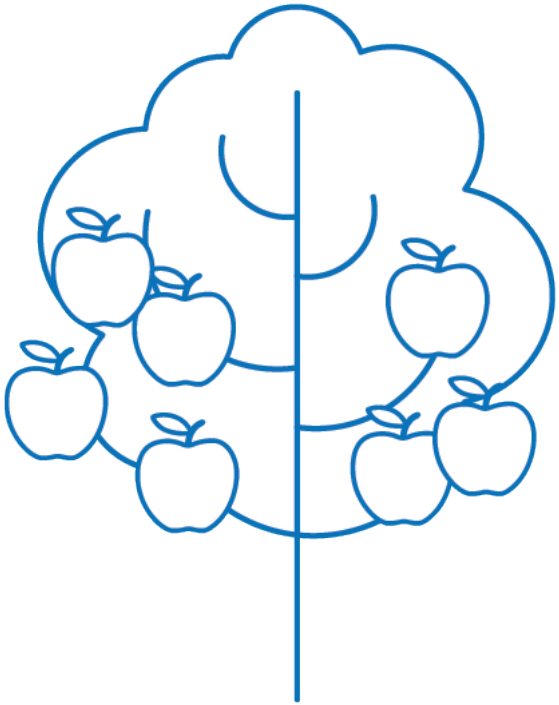
In June 2016 MS-ISAC became aware of a malicious email campaign targeting attorneys, which spoofs emails from statewide legal organizations, such as the Bar Association and the Board of Bar Examiners. The subject and body of the emails include claims that "a complaint was filed against your law practice" or that "records indicate your membership dues are past due." Recipients are asked to respond to the claims by clicking a link which leads to a malicious download, potentially ransomware.

The emails are well written and appear to originate from the appropriate authority, such as an Association official, likely increasing their effectiveness. Reporting from various states indicates a likelihood that this campaign is personalized to individuals practicing in a particular state and may be progressing on a state-by-state basis. The following states have been referenced in public reporting on this campaign: Alabama, California, Florida, Georgia, and Nevada. This targeting may include attorneys working for state, local, tribal, and territorial (SLTT) governments.

Recommendations:
MS-ISAC recommends the following actions:

- Share this information with potentially impacted organizations your area of responsibility, including Departments of Law/Justice, related law enforcement agencies, and agency-specific offices of counsel.
- Train government legal professionals in identifying spear phishing emails which may include spoofed email addresses, unusual requests, and questionable and/or masked links. This particular series of emails includes what appears to be a link to the state bar association, but when the user hovers over the link it shows that the link is really to a different website. Copying and pasting the link, instead of clicking on it, would defeat this social engineering attempt.
- Perform regular backups of all systems to limit the impact of data loss from ransomware infections. Backups should be stored offline.

What Can You Do?



1. PATCH!
2. Use defensive software
3. Train users
4. Enforce passwords standards & 2FA
5. Have frequent, complete, off-line, off-site, and tested back-ups
6. Create a culture where it's OK to ask
7. Work with your ISAC Partners

MS-ISAC 24x7 Security Operations Center

1-866-787-4722

SOC@cisecurity.org

info@msisac.org

Kyle Bryans
Program Specialist
MS-ISAC
518.880.0747
Kyle.Bryans@cisecurity.org