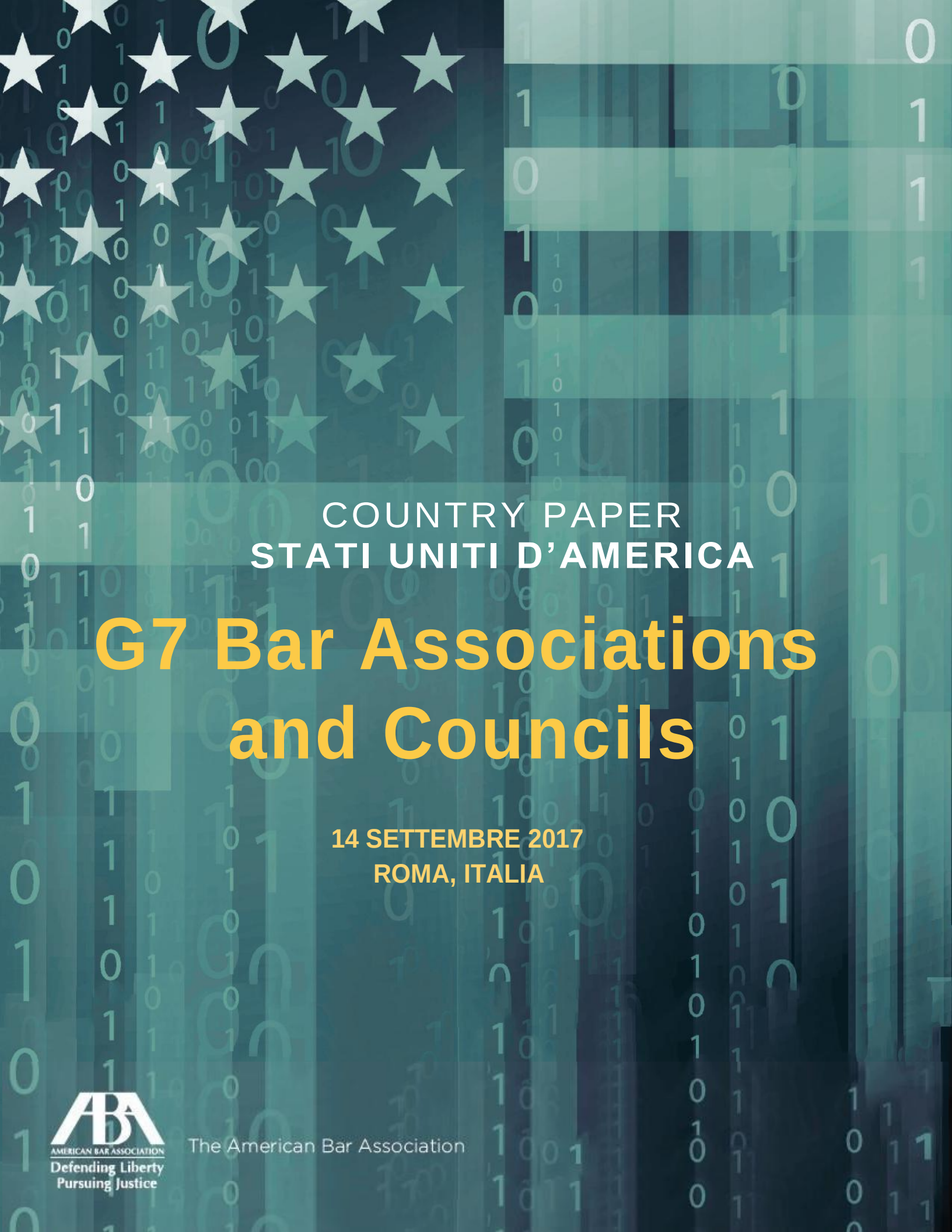

COUNTRY PAPER

STATI UNITI D'AMERICA

G7 Bar Associations and Councils

14 SETTEMBRE 2017
ROMA, ITALIA

AMERICAN BAR ASSOCIATION
Defending Liberty
Pursuing Justice

The American Bar Association

INTRODUZIONE

Come abbiamo visto, il terrorismo informatico è una minaccia estremamente grave per la sicurezza della nostra nazione e stiamo registrando un livello di sofisticazione molto più alto che mai. Le minacce alla cybersecurity sono sempre più volte ad individuare le informazioni sui cittadini e sulle risorse critiche di sicurezza economica e nazionale. Di conseguenza, la sicurezza della nostra infrastruttura digitale è una priorità nazionale per i leader sia nel settore pubblico che privato.

I crescenti attacchi di cybersecurity contro gli enti pubblici e privati statunitensi minacciano la fornitura di servizi essenziali per i cittadini, la sicurezza dei dati aziendali, inclusi i diritti di proprietà intellettuale e commerciale, i beni e dati statali degli Stati Uniti e informazioni personali di identificazione dei cittadini. Dal momento che gli attacchi di cybersecurity si sono evoluti, i leader del settore pubblico e privato sono stati sfidati ad affrontare efficacemente le minacce alla sicurezza della cybersecurity, essendo procedimenti più vecchi di dieci anni. Con le minacce in materia di cybersecurity che mirano allo stesso modo ai settori pubblici e privati, la legislazione e la politica devono portare nuovi e senza precedenti livelli di collaborazione pubblico-privato in un grande gruppo di stakeholder compresi tutti i livelli di governo, delle corporazioni, della comunità legale, dell'università e della cittadinanza.

La Task Force legale della Cybersecurity dell'American Bar Association fornisce la leadership e la competenza degli avvocati al fine di acquisire le competenze in materia di sicurezza informatica e aiuta a capire come proteggere le informazioni dei clienti dalle violazioni della sicurezza in rete. Il gruppo esamina anche i rischi riguardanti i criminali, i terroristi e le nazioni che sperano di rubare informazioni personali e finanziarie, distruggere l'infrastruttura critica e impegnare un nuovo tipo di guerra su un campo di battaglia di "ones and zeros". Composta da membri ABA con competenze in materia di cybersecurity, oltre che rappresentanza del governo, del settore tecnico e privato, la Task Force funge da centro di scambio sulle attività di cybersecurity, sulle migliori pratiche, sulle proposte di politica, il patrocinio e le risorse.
Al fine di impegnarsi efficacemente nel dialogo nazionale in corso in materia di cybersecurity, l'American Bar Association ha approvato la seguente serie di linee guida per le determinazioni delle politiche pubbliche statunitensi per migliorare la sicurezza della cybersecurity. È nostra speranza che questo si rivelerà prezioso poiché i leader delle associazioni di categoria considerano la politica pubblica internazionale utile per migliorare la sicurezza della cybersecurity.

AMERICAN BAR ASSOCIATION

TASK FORCE LEGALE IN TEMA DI CYBERSECURITY

RISOLUZIONE

DELIBERATO che l'American Bar Association invita i rami Esecutivi e Legislativi a prendere in considerazione i seguenti principi guida durante tutto il processo decisionale nel formulare le decisioni politiche statunitensi per migliorare la cybersecurity per i settori pubblici e privati degli Stati Uniti:

Principio 1: Le strutture pubbliche e private sono essenziali per proteggere con successo gli asset, le infrastrutture e gli interessi economici degli Stati Uniti dagli attacchi alla cybersecurity.

Principio 2: La robusta condivisione delle informazioni e la collaborazione tra le agenzie governative e l'industria privata sono necessarie per gestire i rischi cyber globali.

Principio 3: Le strutture legali e politiche devono essere modernizzate per rimanere al di sopra o, perlomeno, tenere il passo dei progressi tecnologici.

Principio 4: La privacy e le libertà civili devono rimanere una priorità nello sviluppo della legge e della politica in materia di sicurezza.

Principio 5: La formazione, l'istruzione e lo sviluppo della forza lavoro delle dirigenze governative e aziendali, degli operatori tecnici e degli avvocati richiedono un investimento adeguato e risorse perché la sicurezza informatica abbia successo.

RELAZIONE

L' American Bar Association riconosce la crescente necessità di azione in risposta ai crescenti attacchi della cybersecurity contro gli enti pubblici e privati statunitensi che minacciano la fornitura di servizi essenziali ai cittadini, la sicurezza dei dati aziendali, inclusi i diritti di proprietà intellettuale e segreti commerciali, e informazioni personali di identificazione dei cittadini. L'uso diffuso di Internet e della tecnologia dell'informazione nel corso dell'ultimo decennio ha creato opportunità senza precedenti. Gli usi nuovi e innovativi di Internet e della tecnologia dell'informazione hanno migliorato la fornitura di beni e servizi essenziali, hanno migliorato la qualità della vita, offrono nuovi modi di connettersi con i cittadini e hanno aperto la strada alla crescita economica di tutto il mondo. Tuttavia, insieme a nuove funzionalità, l'uso di Internet e delle tecnologie dell'informazione può introdurre opportunità per i criminali, i terroristi e gli stati nazionali per minare la fornitura di queste straordinarie capacità e creare rischi di sicurezza nazionali ed economici.

In questo contesto, la sicurezza informatica della nostra infrastruttura digitale è una priorità nazionale per i leader sia nel settore pubblico che privato. L'American Bar Association ha un ruolo fondamentale da svolgere nel promuovere la cybersecurity. L'American Bar Association dovrebbe fornire la leadership e la competenza degli avvocati per acquisire e rimanere competenti nella sicurezza informatica e proteggere le informazioni dei clienti dalle violazioni della sicurezza in rete. Inoltre, l'American Bar Association dovrebbe condurre un nuovo dialogo nazionale sulla sicurezza informatica tra la professione legale, in quanto gli avvocati sono attivamente presenti nella consulenza di governi, società private e comunità senza fini di lucro. Gli studiosi giuridici sono altrettanto posizionati nel mondo accademico per condurre discussioni sull'evoluzione delle sfide della sicurezza in rete e, più profondamente, per offrire soluzioni legali e politiche per risolvere nuove e complesse sfide. Infine, l'American Bar Association dovrebbe promuovere principi di politica che promuovono la nostra agenda nazionale verso una maggiore tutela della sicurezza e della privacy, in patria e all'estero.

Questo rapporto fornisce una panoramica delle minacce informatiche, dei rischi condivisi e di nuovi ruoli e responsabilità per i leader del governo, delle corporazioni, della professione legale, del mondo accademico e della cittadinanza. La relazione si conclude con cinque linee guida iniziali per indirizzare il settore privato e gli organi esecutivi e legislativi del governo nello sviluppo di politiche di sicurezza della rete e di lavorare con i leader del settore pubblico e privato.

Minacce Informatiche

Le minacce sofisticate in materia di cybersecurity sono sempre più mirate sia all'informazione dei cittadini, sia ai fondi critici di sicurezza economica e nazionale. Le minacce globali provocate dai criminali, dai terroristi e dagli stati nazionali rappresentano rischi significativi per i dati critici, le infrastrutture, i dati governativi e aziendali, le informazioni personali e la proprietà intellettuale che creano preoccupazioni nei settori della protezione dei consumatori, della privacy e della protezione delle infrastrutture critiche[1]. I crimini informatici non sono solo una minaccia per i sistemi d'informazione, ma anche, nelle mani di un gruppo anarchico, di un terrorismo o di un gruppo o di una nazione ostili a beni materiali, le comunicazioni necessarie per una società funzionante, processi politici come le elezioni e la vita umana**.**

Sia il governo che il settore privato hanno mostrato una preoccupazione per le minacce alla cybersecurity, i rischi e le potenziali conseguenze, come dimostrato da importanti investimenti del governo e del settore privato nell'infrastruttura della cybersecurity. Tuttavia, gli impegni di risorse da soli non hanno portato ad una attenuazione completa delle vulnerabilità della cybersecurity. Piuttosto, la nazione sta affrontando rischi che richiedono nuovi modi di pensare e competenze per affrontarli.

Rischi condivisi

La cybersecurity minaccia equamente sia i settori pubblici che privati. I settori pubblici e privati condividono anche vulnerabilità comuni, come la fiducia in Internet globale e l'uso di tecnologie moderne per raggiungere clienti e cittadini in tutto il mondo. Di conseguenza, la cybersecurity presenta sia i rischi condivisi che le responsabilità condivise che richiedono ai settori pubblici e privati di affrontare i rischi separatamente e in partenariato.

I leader nazionali hanno trattato la sicurezza in rete e la collaborazione come priorità nazionale e una responsabilità pubblica-privata condivisa per ben oltre un decennio. La Direttiva Presidenziale 63, firmata nel 1998, ha formalizzato i partenariati pubblico-privato come parte chiave della prima politica della nazione in materia di cybersecurity.[2] Da allora, le successive amministrazioni hanno adottato in modo uniforme un approccio collaborativo per la gestione della cybersecurity.

---

[1] Il rapporto annuale 2012 di Verizon Data Breach Investigations ha esaminato 855 incidenti di violazione dei dati dal 2011 e ha scoperto che solo questi incidenti hanno portato a 174 milioni di record compromessi. Verizon, *il rapporto di indagine sulle violazioni dei dati del 2012, disponibile a* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf, (ultima visita 25 settembre 2012). Anche nel 2011, il Dipartimento di Homeland Security ha notato un aumento del 383% degli attacchi alle infrastrutture critiche. Times federali, *Rapporto: gli attacchi di Cyber per infrastrutture critiche salgono nel 383% nel 2011, disponibili a* http://www.federaltimes.com/article/20120703/IT01/307030004/Report-Cyber-attacks-critical-infrastructure-jump-383-2011, (ultima visita il 25 settembre 2012). *Spie straniere rubano i segreti economici degli Stati Uniti nel cyberspazio, il rapporto al Congresso sulla raccolta economica estera e lo spionaggio industriale, 2009-2011; Ufficio del National Counter Intelligence Executive, (ottobre 2011);*www.ncix.gov

2 Decisione presidenziale 63, Protezione delle infrastrutture critiche (maggio 1998). La direttiva presidenziale sulla sicurezza domestica 7 (HSPD-7), l'identificazione, la priorità e la protezione delle infrastrutture critiche (2003); Iniziativa nazionale completa della Cybersecurity, direttiva presidenziale sulla sicurezza nazionale 54 / Direttiva presidenziale sulla sicurezza domestica 23 (NSPD-54 / HSPD-23) (2008); Criterio di Cyberspazio, Assicurare una Infrastruttura di Informazione e Comunicazione Affidabile e Resiliente (2009).

Allo stesso modo, i leader del settore privato e del mondo accademico hanno anche riconosciuto come valore strategico il valore della collaborazione pubblico-privata. Diversi risultati delle principali istituzioni accademiche, dei "think tanks" e delle associazioni professionali richiedono nuovi livelli di collaborazione nei confronti dei rischi condivisi in materia di cybersecurity.

Nuovi Ruoli, Nuove Responsabilità

La nazione richiede livelli nuovi e senza precedenti di collaborazione pubblico-privata. Efficienti strutture richiederanno un ripensamento dei ruoli e delle responsabilità attuali tra i soggetti interessati in vari settori.

- Il governo degli Stati Uniti deve proteggere i dati dei cittadini, nonché i sistemi non classificati e classificati. Inoltre, il governo degli Stati Uniti ha bisogno di sfruttare le sue risorse per mezzo di componenti civili, di applicazione della legge, di difesa, di intelligence e diplomatici per condividere le informazioni sulle minacce e collaborare con il settore privato.

- Le aziende del settore privato che memorizzano o elaborano dati dei cittadini o posseggono e gestiscono infrastrutture critiche dovrebbero continuare a promuovere misure efficaci di sicurezza specifiche per l'azienda e partecipare collaborando con il governo per affrontare le minacce condivise in materia di cybersecurity.

- Gli avvocati hanno una profonda responsabilità (i) per proteggere le informazioni dei clienti e per sviluppare e mantenere sistemi sicuri; (ii) svolgere un ruolo attivo nella creazione e nell'attuazione di strutture pubblico-private; e (iii) rappresentare i clienti che possono sono caduti vittime di crimini informatici.

- L'accademia dovrebbe continuare a partecipare a un dialogo nazionale in materia di diritto, politica e innovazioni tecnologiche. Gli studiosi giuridici, gli amministratori delle scuole di giurisprudenza e altri nella comunità giuridica dovrebbero favorire un ambiente in cui gli studenti di legge possano intraprendere futuri ruoli di leadership e responsabilità in materia di cybersecurity.

- I consumatori ed i cittadini hanno anche ruoli e responsabilità unici e hanno bisogno di risorse migliorate per aiutarli a contrastare e prevenire i rischi della sicurezza in rete.

Principi di Politica Nazionale

La cybersecurity è un problema complesso che richiede un approccio olistico per affrontare i rischi correnti e futuri. L'American Bar Association dovrebbe svolgere un ruolo di leadership nella preparazione degli avvocati per contribuire a questa discussione multidisciplinare e essere disposta a contribuire al dialogo nazionale in materia di cybersecurity. A tal fine, l'American Bar Association dovrebbe adottare i seguenti principi iniziali per guidare il suo ruolo di leadership nel dibattito sulla cybersecurity:

Principio 1: Le strutture pubbliche e private sono essenziali per proteggere con successo gli asset, le infrastrutture e gli interessi economici degli Stati Uniti dagli attacchi della cybersecurity.

Commento: L'avanzare della sicurezza informatica in patria e all'estero richiederà soluzioni che riguardano sia i rischi del settore pubblico che privato. Devono essere sviluppate strutture per definire nuovi ruoli e responsabilità per tutti i partecipanti necessari per garantire la sicurezza in rete. Questi includono i governi a tutti i livelli, le corporazioni, le organizzazioni non profit, le organizzazioni non governative (ONG), gli avvocati, gli accademici ed i cittadini. Questi diversi gruppi devono essere modellati in strutture funzionali che facilitano la cooperazione e contrastino efficacemente le minacce della cybersecurity. Si dovranno studiare nuove strutture di partnership per affrontare minacce informatiche più virulente, mentre le efficienti strutture di partenariato esistenti dovranno continuare a sostenere e partecipare.

Principio 2: La robusta condivisione delle informazioni e la collaborazione tra le agenzie governative e l'industria privata è necessaria per gestire i rischi informatici globali.

Commento: Alla luce della natura globale delle minacce condivise in materia di cybersecurity, sono necessarie forme avanzate di condivisione di informazioni e collaborazione. Le informazioni sulle minacce sono necessarie, ma non sono quasi sufficiente per contrastare i rischi. I settori pubblici e privati devono condividere non solo le informazioni sulle minacce, ma anche le conoscenze su come gestire le minacce alla sicurezza della rete, inclusi strumenti, pratiche e strutture di rischio efficaci. I settori pubblici e privati dovrebbero impegnarsi in un dialogo continuo per consentire loro di condividere costantemente informazioni sulle nuove capacità, sui rischi e sugli sviluppi e su come reagire a loro, pur mantenendo la privacy e la protezione delle libertà civili.

Principio 3: Gli ambienti legali e politici devono essere modernizzati per rimanere avanti o, perlomeno, tenere il passo con i progressi tecnologici.

Commento: Efficaci strutture pubbliche e private per la condivisione di informazioni e la collaborazione richiederanno la modernizzazione della legge e della politica. Al minimo, i settori pubblici e privati dovrebbero esaminare e considerare misure che eliminino ostacoli alla maggiore collaborazione pubblico-privata e alla condivisione delle capacità. La capacità di monitorare e tracciare l'attività criminale e le questioni giuridiche in materia di responsabilità, antitrust e la protezione delle informazioni governative e aziendali rimangono sfide legali che dovrebbero continuare ad essere riviste e considerate. Le scuole legali, ingegneristiche, informatiche e scientifiche dovrebbero sostenere una rigorosa revisione delle dottrine legali e l'applicazione di queste dottrine e offrire soluzioni innovative per contribuire a creare un ambiente giuridico e politico efficace per il prossimo decennio.

Principio 4: La privacy e le libertà civili devono rimanere una priorità nello sviluppo della legge e della politica in materia di sicurezza.

Commento: La privacy e le libertà civili devono rimanere principi fondamentali in quanto la nazione si oppone a minacce e attacchi globali complessi. I legislatori hanno la responsabilità di promuovere nuove forme di collaborazione, ma anche di proteggere e massimizzare la privacy e le libertà civili come parte di queste soluzioni. Poiché i programmi di sicurezza della rete informatica consentono di trasmettere informazioni digitali che potrebbero contenere informazioni personali sensibili o riflettono l'attività protetta dalla costituzione, è fondamentale che questi principi siano fondamentalmente costruiti in programmi informatici fin dall'inizio, e che i programmi informatici siano condotti con ragionevole responsabilità.

Inoltre, la professione legale svolge un ruolo univoco nell'educare i legislatori e il pubblico per quanto riguarda le scelte disponibili, l'impatto di tali scelte e le sfide associate al bilanciamento delle esigenze della cybersecurity nei confronti della privacy e dei diritti di libertà civili.

Principio 5: La formazione, l'istruzione e lo sviluppo della forza lavoro dei dirigenti governativi e aziendali, degli operatori tecnici e degli avvocati richiedono un adeguato investimento e risorse perché la sicurezza informatica abbia successo.

Commento: Le nuove strutture pubbliche e private per la sicurezza informatica richiederanno una forza lavoro addestrata e sostenuta per attuarla e mantenerli. La nazione richiede uno sforzo per sviluppare le competenze in materia di cybersecurity all'interno di tutti i livelli del governo e del settore privato e all'interno della popolazione in generale. L'ABA dovrebbe avere un ruolo fondamentale nell'educare e incoraggiare avvocati, studi legali e cittadini circa la necessità di agire per ridurre al minimo i rischi della sicurezza informatica. Il collegamento più debole può essere il computer di casa individuale che è stato infettato e sta fornendo un ruolo "proxy" (da delegato) nell'attività cybercriminale. Gli avvocati devono dedicarsi a sviluppare costantemente le competenze necessarie per assicurare efficacemente i dati ed i sistemi aziendali e partecipare alle iniziative in materia di cybersecurity con il governo, le corporazioni, la professione legale, gli universitari ed i cittadini.