AIIC 2024 ROMA

Saggezza e Visione nella Cybersecurity

Lee Kim JD CISSP CIPP/US

AIIC associazione italiana ingegneri clinici

Biografia di Lee Kim

- Senior Principal, Cybersecurity and Privacy presso HIMSS
- Avvocato valutato AV Preeminent
- Avvocato autorizzato e avvocato brevettato registrato negli Stati Uniti
- Candidato al consiglio di ISC2
- Corpo Docente di IANS
- Direttore di InfraGard, Regione Capitale Nord
- Membro del Comitato Nazionale di Visita del Centro Nazionale per la Formazione e l'Educazione alla Cybersecurity
- Vice Presidente del Comitato Coordinatore per la Legge Sanitaria e la Politica dell'American Bar Association
- Professionista Certificato in Cybersecurity (CISSP)
- Professionista Certificato della Privacy (IAPP/US)

Bio of Lee Kim JD CISSP CIPP/US

- Senior Principal, Cybersecurity and Privacy at HIMSS
- AV Preeminent rated attorney
- Licensed attorney and registered US patent attorney
- ISC2 Board Nominee
- IANS Faculty
- Director of InfraGard Northern Capital Region
- National Visiting Committee Member of the National Cybersecurity Training and Education Center
- Vice Chair of American Bar Association Health Law and Policy Coordinating Committee
- Certified cybersecurity professional (CISSP)
- Certified privacy professional (CIPP/US)

Cybersecurity nel mondo

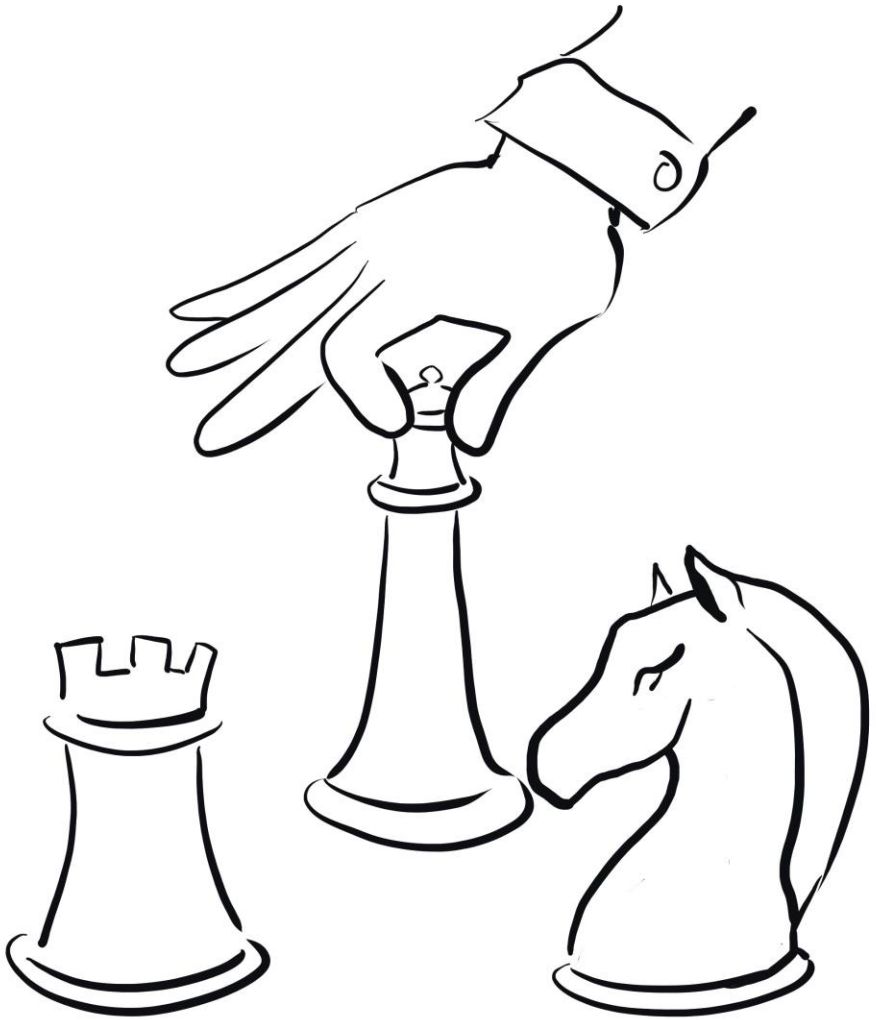
La cybersicurezza è fondamentale

- Cosa ci insegna il mondo sulla cybersicurezza? (Ecco cosa ho imparato in giro per il mondo.)
- **USA**: I soldi non equivalgono a una migliore cybersicurezza. 💵 La preparazione e la condivisione delle informazioni sono importanti**.** ↔
- **Canada**: Governance dei dati e persone. 💼
- **India**: La privacy è un diritto fondamentale. Privacy, riservatezza e accuratezza dei dati. ✔
- **Saudi Arabia**: Standard di protezione e governance dei dati. ⚖
- **Singapore**: L'attacco informatico mirato del 2018 ha portato all'adozione di robuste misure e politiche di cybersecurity. 🎯
- **Indonesia**: La tecnologia dell'informazione sanitaria è nuova e anche la cybersecurity sanitaria è nuova. Ma c'è un grande interesse nell'apprendimento. 🆕
- **Portugal**: Innovazione molto avanzata e strategia di cybersecurity matura, nonché leggi, regolamenti e politiche. 📄 Ricerca cooperativa con il Brasile sul crimine informatico. 🛡

Cybersecurity is Fundamental

- What does the world teach us about cybersecurity? (Here is what I have learned around the world.
- **USA**: Preparedness and information sharing are important.
- **Canada**: Governance of data and people.
- **India**: Privacy is a fundamental right. Privacy, confidentiality, and accuracy of data.
- **Saudi Arabia**: Data protection and governance standards.
- **Singapore**: Targeted cyber-attack of 2018 resulted in robust cybersecurity measures and policies.
- **Indonesia**: Health information technology is new and healthcare cybersecurity is new. But a great interest in learning.
- **Portugal**: Very advanced innovation and mature cybersecurity strategy, and laws, regulations, and policy. Ricerca cooperativa con il Brasile sul crimine informatico.

Strategia di cybersecurity



Strategia di cybersecurity

- La governance è tutto. Senza governance, non hai nulla.
  - Struttura di governance: Ruoli chiaramente definiti; la stessa struttura in tutta l'organizzazione (anche con più strutture).
  - Governance dei dati: Sapere cosa si possiede, dove si trova, chi ha accesso e dove va.
  - Orientamento: Framework di Cybersecurity NIST (attualmente Versione 2.0).
- La preparazione è molto importante. Metti in discussione le tue ipotesi e fai la domanda: E se ciò accadesse?
  - Guida: Effettuare esercitazioni al tavolo (cosa fareste tu e i tuoi colleghi in una situazione; la situazione è scritta in uno script).
- La consapevolezza della situazione (consapevolezza situazionale) è molto importante. Impara condividendo informazioni con altri di cui ti fidi. Impara costantemente - la cybersecurity cambia sempre, soprattutto ora con l'intelligenza artificiale.
- Conosci le priorità - il paziente e la sicurezza del paziente sono le più importanti.
  - Considera sempre - Qual è il rischio per il paziente e per la sicurezza del paziente?
  - Una robusta cybersecurity non dovrebbe avere la priorità rispetto alla cura del paziente.
- L'ingegneria sociale è un grande pericolo – comprendi la psicologia dell'ingegneria sociale e non sarai una vittima.

Cybersecurity strategy

- Governance is everything. Without governance, you have nothing.
  - Governance structure: Clearly defined roles; the same structure across the entire organization (even with multiple facilities).
  - Data governance: Know what you have, where you have it, who has access to it, and where it goes.
  - Guidance: NIST Cybersecurity Framework (currently Version 2.0)
- Preparation is very important. Question your assumptions and ask the question: What if this happens?
  - Guidance: Run tabletop exercises (what you and your colleagues would do in a situation; the situation is written in a script)
- Awareness of the situation (situational awareness) is very important. Learn by sharing information with others whom you trust. Constantly learn – cybersecurity always changes, especially now with artificial intelligence.
- Know the priorities – the patient and safety of the patient are the most important.
  - Always consider - What is the risk to the patient and the patient safety?
  - Robust cybersecurity should not take priority over the care of a patient.
- Social engineering is a great danger – understand the psychology of social engineering and you will not be a victim.

Ingegneri clinici sono eroi

Ingegneri clinici sono eroi

- La sicurezza del paziente è la sicurezza informatica. Dovrebbe essere un diritto fondamentale. Il paziente non è al sicuro a meno che il nostro ambiente non sia sicuro (e protetto informaticamente).
  - L'economia della sicurezza informatica e le priorità della sicurezza informatica (sanitaria) devono cambiare. Dobbiamo essere centrati sul paziente.
- Tutti i dispositivi e i sistemi nella nostra rete devono essere mantenuti da qualcuno. Qualcuno deve assumersi la responsabilità e deve esserci responsabilizzazione.
  - Ospedale
  - Produttore di dispositivi medici (inclusi gli aggiornamenti dei sistemi operativi)
- Qualsiasi cambiamento ai dispositivi, ai sistemi e all'ambiente deve prima essere valutato in termini di rischi e conseguenze.
  - Impatto sul business?
  - Impatto sul paziente?
  - Altri impatti?
- Una volta acquistato un dispositivo medico, dovresti avere anche un piano per sostituirlo; dobbiamo considerare la durata del dispositivo medico e anche l'attualità del sistema operativo del dispositivo medico.
- Gli attaccanti informatici ransomware prendono di mira i sistemi operativi non supportati (legacy).
  - Questo include i dispositivi medici. (Vogliamo evitare il prossimo attacco Wannacry.)
- Orientamento: Protezione dei Dispositivi Medici Legacy

Clinical Engineers as Heroes

- Patient safety is cybersecurity. It should be a fundamental right. The patient is not safe unless our environment is secure (and cybersecure).
  - The economics of cybersecurity and the priorities of (healthcare) cybersecurity must change.
  - We must be patient-centric.
- All devices and systems on our network must be maintained by someone. Someone must take responsibility and there must be accountability.
  - Hospital
  - Medical device manufacturer (including updates of operating systems)
- Any changes to devices, systems, and the environment must first be evaluated in terms of risks and consequences.
  - Business impact?
  - Patient impact?
  - Other impact?
- Once you procure a medical device, you should have a plan for replacing the device too; we have to consider the lifetime of the medical device and also how current the medical device operating system is.
- Ransomware cyber-attackers are going after unsupported (legacy) operating systems.
  - This includes medical devices. (We want to avoid the next Wannacry attack.)
- Guidance: Securing medical devices

Una visione del futuro

Quattro previsioni:

- Avremo una maggiore cooperazione internazionale e assistenza reciproca.
- Il software, l'hardware e i dispositivi saranno auto-rigeneranti (le debolezze verranno automaticamente rilevate e corrette).
- L'intelligenza artificiale aiuterà a facilitare la nostra educazione e la condivisione delle informazioni.
- Gli ingegneri clinici avranno maggiore influenza sulle pratiche di cybersecurity. (La sicurezza del paziente è la cybersecurity.)
- E avremo dispositivi medici più complessi con rischi maggiori ma una maggiore integrazione con l'assistenza al paziente.

Ma non sono solo i dispositivi medici. Dobbiamo assicurarci che tutto il nostro ecosistema sia sicuro. Questo include i nostri ospedali, fornitori, distributori e altri. Tutto è importante.

A Vision of the Future

Four predictions:

- We will have greater international cooperation and mutual aid.
- Software, hardware, and devices will be self-healing (weaknesses will be automatically detected and fixed).
- Artificial intelligence will help facilitate our education and information sharing.
- Clinical engineers will have more influence over cybersecurity practices. (Patient safety is cybersecurity.)
- And we will have more complex medical devices with greater risks but greater integration with patient care.

But it's not just medical devices. We need to ensure that our whole ecosystem is secure. This includes our hospitals, vendors, suppliers, and others. Everything matters.

Domande? Questions?

Lee Kim JD CISSP CIPP/US
www.linkedin.com/in/leekim
Lee.Kim.JD@gmail.com

AIIC 2024 ROMA

Grazie per l’attenzione!

AIIC associazione italiana ingegneri clinici