

CYBERSEC 2024
臺灣資安大會

5/14_{Tue} — 5/16_{Thu}
臺北南港展覽二館

**Generative
Future**

Keynote Session

Essentials for an Aspiring CISO: Leading with Confidence in Uncertain Times



Kyle Lai, *President & CISO*
KLC Consulting

<https://klcconsulting.net/in/kylelai>
cmmc@klcconsulting.net



Kyle Lai

President and CISO KLC Consulting

CMMC-CCA, CCP, RP CISSP, CSSLP, CISA, CDPSE, CIPP/US/G

Biography

<https://www.linkedin.com/in/kylelai>

cmmc@klcconsulting.net

KLCConsulting.net



- 25+ years in IT & Cybersecurity (NIST 800-171, Software Security, Pentest, Third-party Risk, Compliance, Privacy, Engineering)
- Security Advisor to Fortune 500 companies
- Expert in Software, DoD, Financial, Energy, Healthcare, Manufacturing sectors
- Security advisory for Microsoft, PwC, Boeing, HP, Fidelity Investment, ExxonMobil, Zoom, DISA

- DoD Authorized CMMC C3PAO (KLC Consulting)
- Former DISA (DoD) Operations Manager
- Former CISO of Pactera & Brandeis University – Heller School
- Former Penetration Tester for Fortune 500 firms
- Author of SMAC MAC Address Changer – Over 3 million users
- SME on CMMC, NIST 800-171, NIST 800-53, DoD RMF

Agenda

- ❖ CISO Challenges
- ❖ Leadership & Business Acumen
- ❖ Risk Management
- ❖ Technology Adaptation Management

Where Are We?

Cloud environment intrusions
increased by **75%** in one year

– 2024 Global Threat Report by CrowdStrike

39% of companies are
training employees to better
understand the threats posed
by generative AI

– CISO Report 2023 by Splunk

Most common threat vectors:

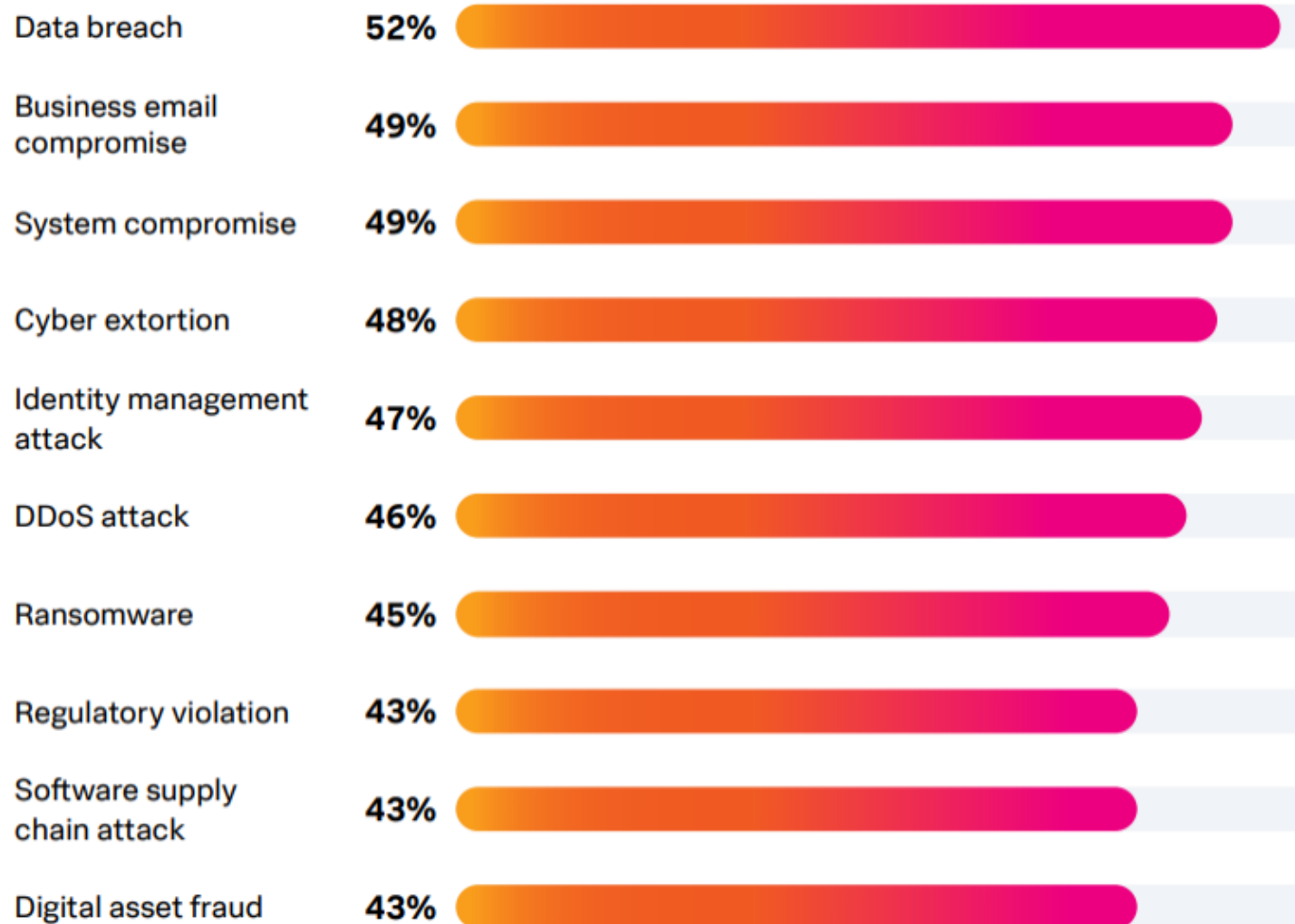
Misconfigured systems **38%**

Vulnerabilities in internally
developed apps **31%**

93% of businesses adopted
AI, but **31%** lack an AI
Security Policy

– State of Security 2024 by Splunk

Most frequent incidents experienced in the past two years



Source: State of Security 2024 by Splunk

Risk Management	Third Party Risk Management	Endpoint Protection	Software Security	Vulnerability Management
Certification maintenance	Internal Audit Response	Configuration Management	Security Awareness Training	Patch Management
Penetration Testing	Cloud Security	Regulatory Compliance	AI Security, Safety, & Trustworthiness	Incident Response
Network Security	Physical Security	RFP / Customer Questionnaire	Identification & Authorization	Zero Trust Architecture

CSO Responsibilities

(Not an exhaustive list)

Words of wisdom

“The only way to do great work is to LOVE WHAT YOU DO.”

– Steve Jobs

CISO Challenges



**Leadership &
Business Acumen**

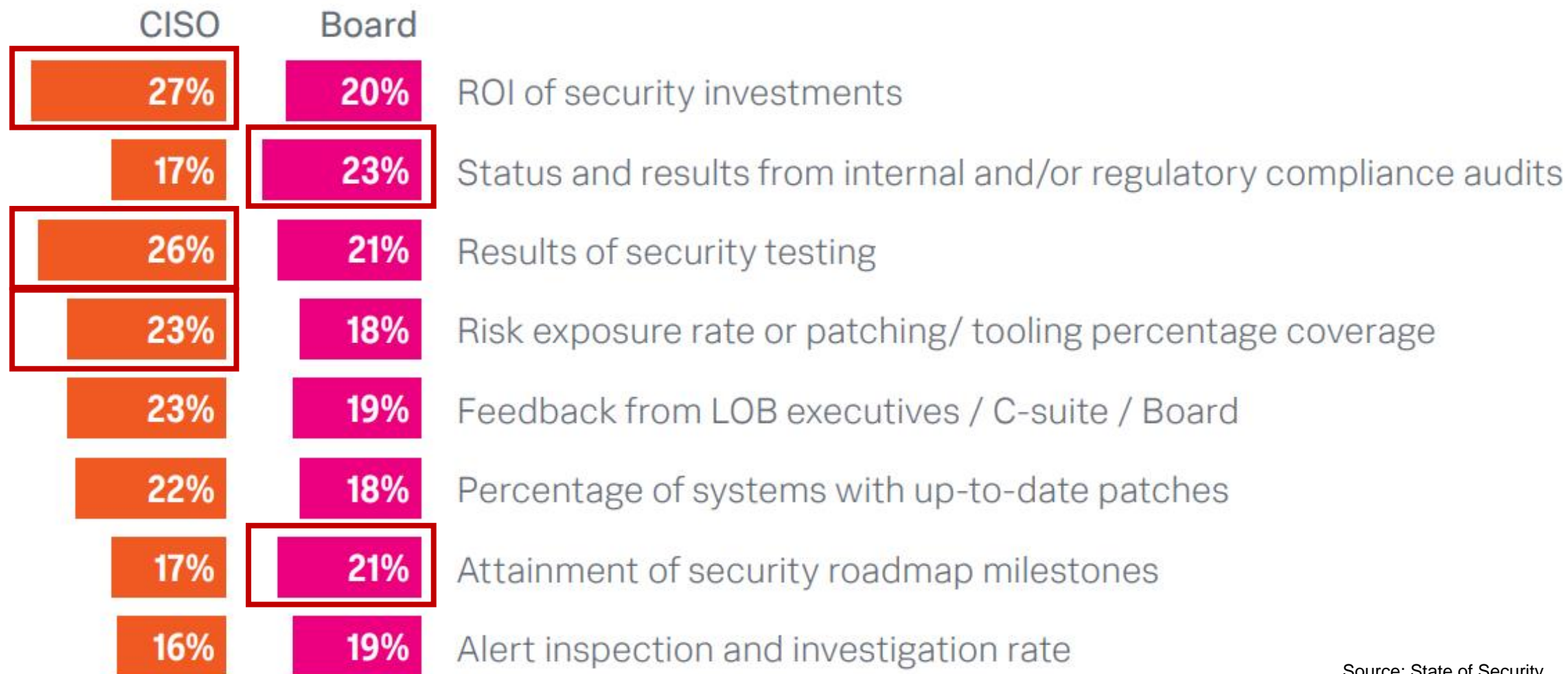


**Risk
Management**



**Technology Adaptation
Management**

Ranking Cybersecurity Program Success Factors



Source: State of Security
2024 by Splunk

Leadership

1

**Know
business
operations**

2

**Build strong
relationships &
trust through
collaboration**

3

**Get mentorship
& provide
mentorship
to staff**

4

**Develop a
culture of
cybersecurity
& learning**

Business Acumen



Financial Knowledge



**Communicate in
non-technical terms**



**Know where you are &
where you need to be**

Risk Management



**Know the
regulations**



**Have a
detailed incident
response plan**



**Establish
cybersecurity
framework
& risk register**



**Supply chain risk
management**

Regulatory Compliance Training

91% of companies are ramping up security training for legal and compliance teams

90% of companies are ramping up legal and compliance training for security teams

91% of companies say everyone on their security team makes compliance a part of their jobs

Source: State of Security 2024 by Splunk

Generative AI-related risks that organizations consider relevant and are working to mitigate, % of respondents¹.

Inaccuracy, cybersecurity, and intellectual property infringement are the most cited risks of generative AI adoption.



Source:
McKinsey & Company

¹Asked only of respondents whose organizations have adopted AI in at least 1 function. For both risks considered relevant and risks mitigated, n = 913.
Source: McKinsey Global Survey on AI, 1,684 participants at all levels of the organization, April 11–21, 2023

Manage Technology Adaptation

**Rapid technology
advancements
(e.g. AI)**

**Work closely with
Business and IT on
new technology
adoptions**

**Ask vendors about
tools to address
new risks**

Future

- ❖ “What doesn't kill you makes you stronger!”
- ❖ CISO will be accountable for security incidents
- ❖ More Regulations will target the CISO role like Sarbanes-Oxley (SOX) for the CFO
- ❖ Ask for Director & Officer (D&O) Insurance Coverage to protect yourself

Calling capable CISOs!

Contact Information



Thank you!

Kyle Lai

President and CISO

KLC Consulting

CMMC-CCA, CCP, RP CISSP, CSSLP, CISA, CDPSE, CIPP/US/G



klai@klcconsulting.net



<https://www.Linkedin.com/in/kylelai>



[KLC Consulting Youtube Channel on CMMC](#)

www.klcconsulting.net

