



LASSITER CONSULTING

330 Beacon Street, Boston MA 02116

Career Management Services

www.lassiterconsulting.com

pam@lassiterconsulting.com

617-267-7105 (T) 617-267-6111 (F)



Are You Protecting Your Corporate Crown Jewels?

by Pam Lassiter, www.lassiterconsulting.com

Interviewing Maria Kussmaul, Head of the IT Security Practice at AGC Partners, about the CEO's role in cyber risk management was a true education for me

<http://www.lassiterconsulting.com/ceoacademy.html>. It's not just the IT Department's job any more; the enterprise is at stake. You've heard enough about millions of accounts stolen from Yahoo, credit cards from Target, money being siphoned from bank accounts, and East Coast websites from Airbnb to Zillow crashing due to a malware attack to know that anything can be invaded now, including the government and defense systems.

So what's a CEO to do? Start with knowing your Board's concerns:



"Cyber Risk Oversight," Director's Handbook Series, National Association of Corporate Directors, 2017 <https://www.nacdonline.org/cyber> (permission granted for use)

Principle 1

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, *not* just as an IT issue.

Principle 2

Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

Principle 3

Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.

Principle 4

Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

Principle 5

Board-management discussions about cyber risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

The CEO's role becomes clear as the one who sets the strategy, is clear on the risks and has different levels of protection around corporate assets with the highest being around your "crown jewels", and continually works with the Board, IT, external stakeholders and the company to ensure that all practices and policies reflect current and future-oriented approaches. Listen to <http://www.lassiterconsulting.com/ceoacademy.html> for more details.