ADVICE FROM AROUND THE GLOBE:
WHAT AMERICAN CISOS SHOULD LEARN FROM INTERNATIONAL EXPERTS

CISOs always want to have the answer, even though they are in an emerging and rapidly changing industry. One of the most valuable things is to remember there are always questions or challenges that CISOs are just not well-versed on because they have not had the experience yet.

There is still so much to learn from CISOs across around the globe, who are innovating security solutions to very stringent data privacy issues, tackling cyber security threats from locally-based but globally focused cyber terrorists, and routinely working to address security challenges outside their own country's borders. Here are some tips for CISOs from experts based outside of the United States.

Trust is a Security Necessity

"At the centre of a global financial institution must be trust. Trust is a differentiator for the modern customer, and in a hyper connected world customers will need to know and demand, that their most sensitive personal information on i.e. identity, address, salary, mortgage, credit card spends, pension, travel, shopping habits are kept safe."

- Troels Oerting, CISO Barclays (Linkedin blog post)

Public-Private Partnerships Spurs Innovation

"The government's role in Japan's cybersecurity without limiting the growth of the technology market ... that will drive innovation."

- Danielle Kriz writes in The New America Weekly, quoting Intel's Mihoko Matzubara

Pay Attention to ICS

"Cybersecurity of ICS should not be handled by the CIO or the CISO because that team typically knows technology, not engineering. The CISO should work with, not over, the engineering team to make sure cyber is addressed in these critical systems. Singapore, a major petro-chemical shipping port, is one of the first regions that is starting to understand the difference between ICS cybersecurity and operational cyber security. We can find examples of best practices in how the government of Singapore is approaching the problem."

- Control Systems cybersecurity expert, Joseph M. Weiss

Data Privacy Officers Must Play Critical Roles

"The DPO is, or should be, a "C Suite" person who has direct reporting to the management in respect of data privacy and related compliance issues. The DPO shall have the autonomy and related budget and decision-making powers to manage non-compliance and related events including reporting of such incidents to the relevant DPA."

- Robert Bond, of the UK law firm Charles Russell Speechlys

The CEO is Head of Security

"It is appropriate for the CEO to lead a crisis response, should a major attack arise. But cyber security should sit with someone able to take full day-to-day responsibility, with Board oversight, and who can be fully sanctioned if the company has not taken sufficient steps to protect itself from a cyber-attack. To ensure this issue receives sufficient CEO attention before a crisis strikes, a portion of CEO compensation should be linked to effective cyber security, in a way to be decided by the Board."

- According to the UK Culture, Media and Sport Committee's report *Cyber Security: Protection of Personal Data Online*