DETERMINING LIABILITY

IS NOW BEING DEFINED BY THE COURTS

When should a company be considered negligent in its processes of securing sensitive information?

1

CARELESS?

Should an enterprise or third-party provider be liable for not addressing common, vulnerabilities?

REAL WORLD EXAMPLES

The JPMC Corporate Challenge charity website and British telecom provider TalkTalk were apparently breached through a common application-layer vulnerability called SQL Injection, which has been on the OWASP Top 10 list of most critical vulnerabilities for more than a decade.

2

UNPATCHED?

Is it a "standard of due care" to patch published vulnerabilities such as Heartbleed?

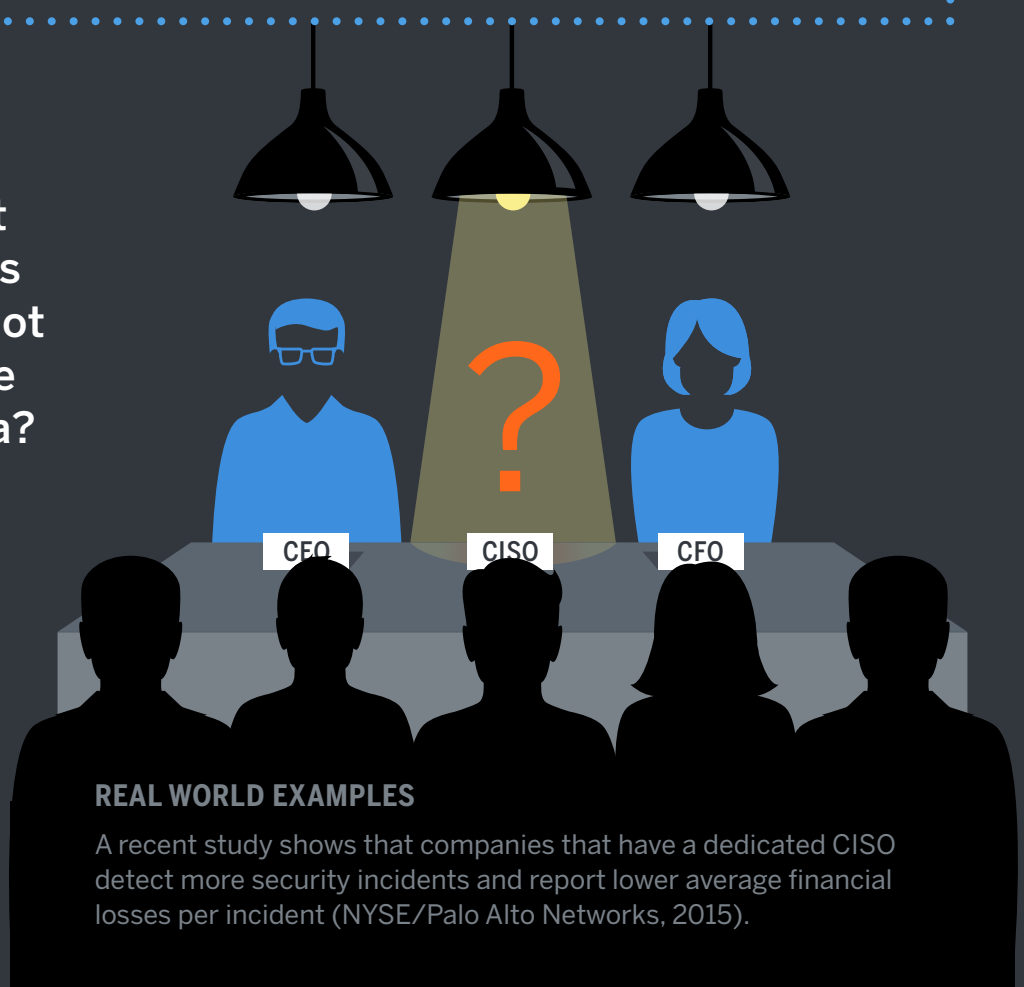
REAL WORLD EXAMPLE

Verizon 2015 Data Breach Investigations Report shows that 99.9% of the software vulnerabilities exploited were publicly announced more than one year before they were exploited.

3

NO CISO?

Can we assume that a company that does not have a CISO is not making a reasonable effort to secure data?



REAL WORLD EXAMPLES

A recent study shows that companies that have a dedicated CISO detect more security incidents and report lower average financial losses per incident (NYSE/Palo Alto Networks, 2015).

NYSE GOVERNANCE SERVICES, IN PARTNERSHIP WITH VERACODE

VERACODE NYSE