PULSE kiuwan

Cybersecurity Risk Management

Cybersecurity risk management is a framework that enables businesses to identify, quantify, respond to, and mitigate risks to their digital infrastructure and assets from external and internal threats. Identifying cybersecurity vulnerabilities and their potential impact is critical for businesses becoming increasingly digitized. Cybersecurity breaches can be damaging not only to an organization's infrastructure but also its long-term reputation. IT leaders, particularly CISOs/CSOs, are usually tasked with translating cybersecurity threats to non-technical business leaders. Is the business ready to listen to, and budget for, IT's concerns?

In this One-Minute Insight Report, Pulse asked over 100 IT leaders:

- About current risk management infrastructures and budgetary plans
- How the business approaches risk and their own ability to communicate risk
- Where the blame for breaches ultimately falls

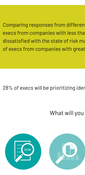
Data collected from Dec 18, 2020 - Jan 5, 2021

Total Respondents: 120 IT executives

Most execs have a satisfactory cybersecurity risk management framework, and budgets are set to increase

61% of execs report that their organization has a framework for quantifying cybersecurity risk.

Overall, 61% of execs are expecting their risk management budget to increase over the next 3 months, with most reporting an 11-15% increase (26%).



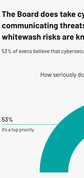
Overall, 83% of execs are satisfied with their organization's risk management.

Comparing responses from different sized companies, 22% of execs from companies with less than 1K employees were dissatisfied with the state of risk management, compared to 9% of execs from companies with greater than 10K employees.

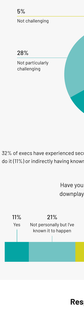
28% of execs will be prioritizing identifying risks in the next 3 months.

No blame for breaches—execs trust themselves to identify risk, and no single office should be held responsible when breaches occur

Overall, 86% of execs believe in their own ability to identify risk.



While many execs preferred not to blame a single office for security breaches (46%), over a quarter said the blame should be directed at the CISO/CSO's office (27%).



Risk management cultures involve open dialogues and over a third of execs are using software for their frameworks

46% of execs describe their risk culture as a mix of rules and open dialogue, while 18% report the culture as rules-based only.

35% of execs currently use enterprise risk management (ERM) software to quantify risk.

The Board does take cybersecurity risk seriously but communicating threats isn't easy—and pressures to whitewash risks are known

53% of execs believe that cybersecurity is a top priority for their board of directors.

However, 67% of execs overall find it challenging to communicate risk to the business.

32% of execs have experienced security risk 'whitewashing', either directly having been asked to do it (11%) or indirectly having known it to happen (21%).

Respondent Breakdown