

MITIGATE CYBER RISK WITH SECURITY PERFORMANCE MANAGEMENT



Sponsored Content

Businesses need a new weapon in the fight against cybercrime. Despite the best efforts of security teams, spending is up on protection, but with minimal advances to show for it.



SPENDING HAS INCREASED ANNUALLY FOR SECURITY



Worldwide spending on information security products and services is forecasted to grow 8.7% to

\$124 BILLION

according to Gartner



Forrester found

28%

of U.S. private-sector IT budgets are spent on cybersecurity



58%

of organizations will increase cybersecurity spending in 2019, according to ESG

DESPITE THIS INCREASED SPENDING, BREACH RATES AND COSTS ARE UP



Ponemon Institute reports a typical **data breach costs** a company \$3.86 million, up 6.4% from

\$3.62 MILLION YOY



TWO-THIRDS

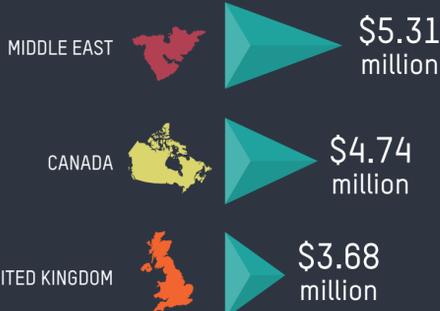
of organizations experienced an average of **five or more security breaches** in the past two years, according to Forrester



U.S.-based breaches are the most expensive, on average

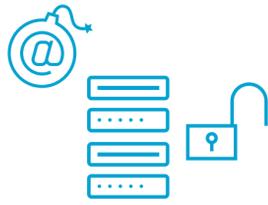
\$7.91 MILLION

OTHER BREACH COSTS BY REGION:



GLOBAL ACCOUNTABILITY AND COMPLIANCE DEMANDS ARE RAMPING UP

The legislative landscape demanding accountability from organizations is heating up, most recently with the European Union's [General Data Protection Regulation \(GDPR\)](#).



Since the GDPR came into effect in May of 2018, EU organizations have reported almost

60,000 DATA BREACHES

OTHER SIGNIFICANT GLOBAL REGULATIONS:



- ✓ Health Insurance Portability and Accountability Act (HIPAA), U.S.
- ✓ Family Educational Rights and Privacy Act (FERPA), US
- ✓ Data Protection Act, UK
- ✓ Criminal Justice Information Services (CJIs), U.S.
- ✓ NYDFS Cybersecurity Regulation (23 NYCRR 500), U.S.

IN 2018:



U.S. states considered more than

265 BILLS

related to cybersecurity



52 OF THOSE BILLS

were enacted



According to IDG research

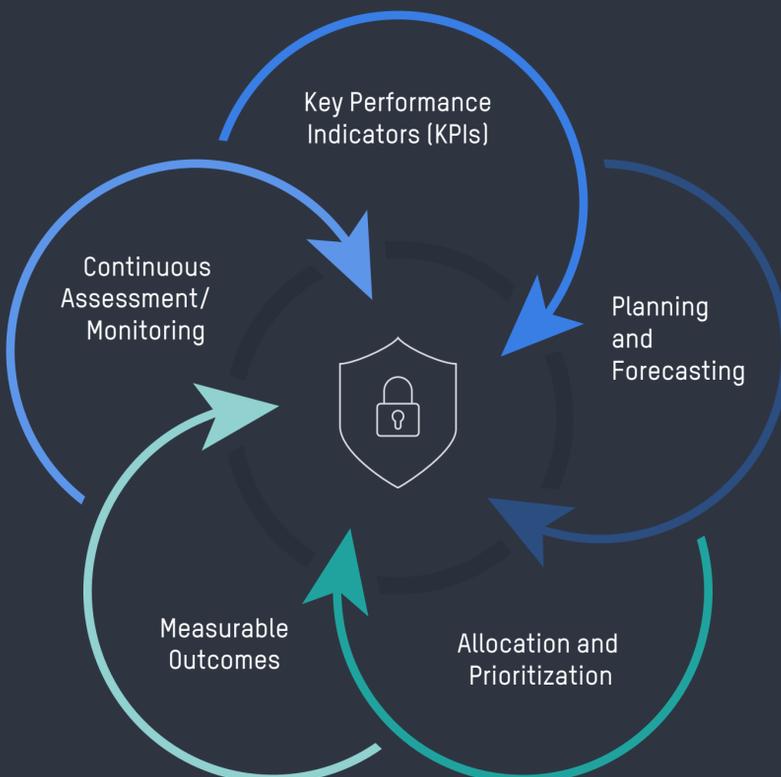
58%

of top security executives brief the board at least quarterly

Board oversight and demands on cybersecurity are common now

SECURITY PERFORMANCE MANAGEMENT (SPM) FILLS IN THE GAPS

Accountability is now key in security—and businesses need a reliable way to measure, monitor, and manage security performance. That is done with SPM, which includes:



BITSIGHT

BitSight for Security Performance Management helps security and risk leaders take a risk-based, outcome-driven approach to managing the performance of their organization's cybersecurity program through broad measurement, continuous monitoring, and detailed planning and forecasting in an effort to measurably reduce cyber risk.

Learn more at www.bitsight.com