The State of Cybersecurity and Digital Trust 2016

In the digital business environment, trust is built on two components: ethics and security. Consumers not only expect cybersecurity; they demand it in today’s trust-based digital economy.

Many threats to data come from within. External threats are a rising concern. Digital transformation is having a major impact. Customer-facing threats are increasing.

For almost half (49%) of respondents, organized crime or professionals are the external threats of most concern. That of respondents said digital capabilities are having a strong to critical impact on data security.

The business goals identified as most vulnerable to data security gaps were brand reputation (43% of respondents) and customer support (36%).

The most significant expected increase was a 62% hike in data theft or corruption of corporate information by insiders.

The State of Cyber Threats
Significant and Diverse
The “State of the art” in cyber defense is evolving as digital technologies proliferate and professional threat actors increase.

In the digital business environment, trust is built on two components: ethics and security. Consumers not only expect cybersecurity; they demand it in today's trust-based digital economy.

The State of Cyber Response
Five Cybersecurity Gaps Undermining Digital Trust

Talent Gap
Between the technical and operational staff required and the pool of available talent.

Technology Gap
Between the growth of cyber threats and the ability to quickly deploy and leverage new technologies to secure business initiatives.

Party Gap
Between cyber propensities and threats among regions, verticals and partners in the extended enterprise.

Budget Gap
Between the budget required and available funds—a gap fueled by financial realities and management focus.

Management Gap
Between executive management and security operations’ perceptions of cybersecurity in the extended enterprise. This gap, if widened, can lead the way to closing the other gaps.

TALENT GAP
GAP 54% indicated their employees are underprepared to prevent security breaches.

TECHNOLOGY GAP
GAP The largest growth was anticipated in emerging technologies to mitigate advanced threats to data. In 2014, cognitive computing (43%), biometric authentication (43%), behavioral tracking (25% increase), and automation (21% increase).

PARTY GAP
GAP 35% believed management is unconcerned with security, and 36% believed management considers security an unnecessary cost.

BUDGET GAP
GAP On average only 35-57% of partners were reported to be cyber vetted, placing most enterprises at considerable risk. And anticipated 41-51% improvement in vetting still leaves gaps.

MANAGEMENT GAP
GAP 62% indicated that the biggest inhibitor to securing their enterprise is budget-related.

OPPORTUNITY
Acquire top talent, develop talent through effective training and testing, and establish business partnerships. Collaboration is critical.

OPPORTUNITY
Adopt a long-range strategy of budget and talent expansion, coupled with a conceptual-test-implement-refine methodology.

OPPORTUNITY
Tightly link cybersecurity to—or embed it in—risk management and digital functions to obtain optimal funding.

OPPORTUNITY
Acquire, train and develop security talent.

OPPORTUNITY
Foster an enterprise culture of corporate and personal data responsibility and security.

OPPORTUNITY
Strengthen security partnerships with all providers.

OPPORTUNITY
Set security priorities consistent with business goals.

OPPORTUNITY
Increase collaborative security operations and management.

OPPORTUNITY
Develop innovation and testing capabilities.

OPPORTUNITY
Change how cybersecurity funding is viewed.

Cybersecurity professionals must work with business units, executives, and all employees, partners and customers—all members of the extended enterprise—to sustain an environment of digital trust and protect the success of the digital business.

The Future Depends on Talent, Leadership Focus, and Budget
Actions to foster a culture of cybersecurity awareness and enhance digital trust

High performance. Delivered.