accenture

HfS Research

The State of Cybersecurity and Digital Trust 2016

Identifying Cybersecurity Gaps to Rethink State of the Art

Executive Summary

Executive Summary

While the advent of digital technology has fueled new business models and opportunities, it has also brought an element of risk as valued assets become less tangible, more distributed, and more vulnerable to cyber threats.

Today, many different types of cyber attackers threaten organizations, from individuals working alone ("lone wolves") to highly organized, well-sponsored teams-for-hire capable of breaching the most sophisticated cybersecurity systems target personal, corporate or state secrets.

Cybersecurity today must include a rethinking of the nature of security, and a shift from an approach that stresses protecting vulnerable assets to one based upon strengthening assets, making them more resilient as part of a holistic cybersecurity process that delivers greater value to the enterprise.

Cybersecurity needs to be part of a larger value framework that includes both risk management and the development of digital trust.

Digital trust is not a technology, nor a process—it's an outcome exemplified by secure, transparent relationships and engagement between the enterprise and its employees, partners, and customers. It is driven by how information and data assets are both secured and used, and it's what helps keep a digital brand memorable and successful.

But how can a company achieve this in an environment where state-of-the-art technology and tactics are often at a disadvantage against an adversary engaged in asymmetrical cyber tactics? It requires focusing not on technology state-of-the-art, but instead on state-of-the-art as an organizational mindset, one that continually evolves and adapts to counter evolving threats. It requires a leadership-driven cybersecurity culture throughout the enterprise ecosystem. And it requires a holistic security approach that results in shared "digital trust" and greater value for all stakeholders.

Research shows a number of key gaps that both cybersecurity professionals and business executives must close to build a successful digital enterprise in the trust-based economy. These gaps include deficiencies in five key areas: talent; technology (detection and response); organizational parity; budgets and funding; and management.

But cybersecurity is still a young profession—the current role of the chief information security officer (CISO) is barely a decade old—and the idea of "digital trust" as a foundation of business success is still an emerging concept in the digital economy.

In March 2016, HfS Research and Accenture surveyed 208 enterprise security professionals across a range of geographies and vertical industry sectors. Our key objective was to learn how cybersecurity threats are both perceived and countered within the enterprise, with a goal of understanding both the current state of cybersecurity and the steps the enterprise must take to better enable digital trust throughout the extended ecosystem.

The results of the Accenture and HfS cybersecurity survey are sobering: cybersecurity leaders do not believe the threats are going away—in fact, they expect them to increase and continue to impact, or act as an inhibitor to, achieving enterprise-wide digital trust. While making investments in basic technology defenses such as firewalls, and new technology such as behavioral analytics tools, organizations simply do not have enough skilled professionals to leverage security technology properly. There are clearly gaps between where most enterprises are and where they feel they need to be. And yet, 36 percent of respondents believe that executive management views cybersecurity expenditures as an unnecessary cost.

Many cybersecurity teams are attempting to close the gaps that exist, experimenting with advanced cognitive and other artificial intelligence technologies, while still struggling to find the security talent to execute on the basics effectively. Establishing digital trust, which is seen as crucial to competitive success, clearly requires a new mode of working, not simply incremental improvement.

Key findings of the study include the following:

The State of Cyber Threats

- Data theft of "corporate information by outsiders" and the theft of "personal information by corporate insiders" dominate the discussion, with 35 percent of respondents indicating they were strongly or critically concerned about these two threats over the past 12 months. But moving forward, overall data loss or destruction becomes a top rated concern, with 41 percent of respondents indicating strong or critical concern over the coming 12 to 18 months.
- The threat sources of most concern to enterprise security professionals are private, well-organized teams, organized criminals, and state-sponsored professionals with agendas of corporate espionage and the targeting of critical infrastructure as their main concerns.
- Brand reputation and customer support are rated the most vulnerable business goals, with 43 percent and 37 percent (respectively) of respondents listing data security as critically important to supporting those efforts.
- Cloud computing, a culture of cybersecurity awareness, and cloud storage are rated as the most important enterprise initiatives, while mobile tops the list of initiatives at risk, with 47 percent of respondents listing a data breach or loss of service involving mobile as having the highest risk to the enterprise brand.
- Sixty-nine percent of respondents have witnessed an attempted or realized data theft or corruption by corporate insiders, with media and technology firms and enterprises in the Asia-Pacific region reporting the highest rates (77 percent and 80 percent respectively).

Digital trust is more important than ever and cybersecurity is not only expected by consumers, it's demanded in today's trust-based digital economy.

"In today's digital business environment, trust is built on two major components: ethics and security. Trust is the cornerstone of the digital economy."

Source: Accenture Technology Vision 2016 Survey, People First: The Primacy of People in the Digital Age www.accenture.com/technologyvision, #techvision2016

The State of Cyber Response

FIVE GAPS UNDERMINING DIGITAL TRUST

TALENT GAP

- Cybersecruity teams are struggling, with 42 percent of respondents believing that while they have enough budget for security technology, they need additional budget for hiring security talent and training. Thirty-one percent of respondents list lack of training or staffing budget as their single biggest inhibitor to cybersecurity readiness.
- Only 20 percent of respondents believe their managed security services provider (MSSP) is a true partner who leads through innovation, while 31 percent believe their MSSP could offer more innovation.
- Seventy-six percent of respondents believe they need some level of improvement in their ability to conduct threat and vulnerability assessments, while an additional 24 percent consider themselves to be state-of-the-art.

TECHNOLOGY GAP

- Enterprises are relying on the same standard technology, such as firewalls and encryption, to combat cyber threats, but the hottest growth areas are cognitive/AI, data anonymization, behavioral tracking, and automation—areas that involve new spend and new skills.

PARITY GAP

- Differences between different enterprise units and functions continue to exist, with IT teams being rated the most secure and sales teams rated the least secure (with 25 percent of respondents stating their sales force is either not very or only somewhat secure).
- Between 35 percent and 57 percent of enterprises say they vet ecosystem partners for cyber-integrity and preparedness, with BPO partners being the least vetted and credit partners being the most vetted.
- Differences in cyber preparedness among business units, geographies, and vertical industries continue to demonstrate that not all ecosystem partners are at the same level of cybersecurity preparedness.

BUDGET GAP

- Seventy percent of respondents cite a lack of, or inadequate, funding for either cybersecurity technology or security talent (including training).
- An additional 12 percent of respondents state they have inadequate funding/staffing levels or are being asked to cut back.

Failure to proactively address these gaps could significantly weaken enterprise security, slowing cybersecurity maturity and leading to increased enterprise risk.

MANAGEMENT GAP

- While 54 percent of respondents agree or strongly agree that cybersecurity is an enabler of digital trust for consumers, 36 percent believe their executive management considers cybersecurity an unnecessary cost.
- Large enterprises (greater than 50,000 employees) have the largest percentage of cybersecurity professionals who believe management views cybersecurity as an unnecessary cost (48 percent), a number matched within public sector/government/non-governmental organizations.
- Only a third (36 percent) of cybersecurity professionals have a direct reporting line to the CEO, with cybersecurity professionals anticipating a shift in reporting structure away from the CEO and CIO in favor of the COO and chief risk officer (CRO).
- Only 5 percent of respondents' organizations have a chief risk (or trust) officer who reports directly to the CEO or board of directors.

State-of-the-art in cybersecurity is an approach, a mindset—not an implementation or technological end-state. It evolves and adapts as the value of assets shift and the type or level of threat changes.

Key recommendations arising from our analysis of the study results include the following:

Executive management must assume a visible, vocal, and engaged position on cybersecurity, driving a culture that values and leverages enterprise-wide digital trust.

Existing cybersecurity talent must be expanded and trained, leveraging holistic security practices and emerging technologies to better address the number and sophistication of cyberattacks.

Cybersecurity operations and executive management must collaborate to identify and close gaps between security requirements and execution ability in areas such as talent and training; technology and process; and budgets and finance, with an eye toward ensuring a high level of enterprise-wide security preparedness.

Enterprise cybersecurity teams must establish innovation and testing capabilities to rapidly and cost-efficiently identify, vet, and test new and emerging technologies (such as behavioral analytics, automation, cognitive, and physical/digital integration) to keep pace with the evolution of cyber threats.

Enterprises should consider a shift in how cybersecurity funding is viewed, away from treating costs as overhead. Instead, a holistic approach should be followed—one that includes the cost of securing data and allowing it to be used—as part of overall business initiative financial requirements.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 373,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

About HfS Research

HfS Research is The Services Research Company™—the leading analyst authority and global community for business operations and IT services. The firm helps enterprises validate their global operating models with world-class research and peer networking. HfS Research coined the term The As-a-Service Economy to illustrate the challenges and opportunities facing enterprises needing to re-architect their operations to thrive in an age of digital disruption, while grappling with an increasingly complex global business environment. HfS created the Eight Ideals of Being As-a-Service as a guiding framework to help service buyers and providers address these challenges and seize the initiative. HfS facilitates a thriving and dynamic global community of more than 100,000 active subscribers, which adds richness to its research. Visit us at www.hfsresearch.com.

16-2310