ESI THOUGHTLAB

Press release

Contacts:

Lou Celi, CEO, ESI ThoughtLab
Mobile: 917-459-4614
Email: Lceli@esithoughtlab.com

Mike Daly, Communication Specialist, ESI ThoughtLab
Office: 215-717-2777
Email: Daly@econsultsolutions.com

New Global Research Shows that Digital Transformation Heightens Risk of Costly Cyber Attacks

ESI ThoughtLab releases cybersecurity analysis and benchmarks covering 1,300 companies

October 16, 2018 *(Philadelphia, PA)* **–** A comprehensive study about cybersecurity from leading research firm ESI ThoughtLab, together with a cross-industry coalition of organizations including Baker McKenzie, CyberCube, HP Inc., KnowBe4, Opus, Protiviti, Security Industry Association, Willis Towers Watson, and WSJ Pro Cybersecurity shows that digital transformation is exposing companies to higher and more costly cyber risks. According to a global benchmarking study of 1,300 companies, those whose cybersecurity practices do not keep pace with their digital transformation initiatives are more likely to see US$1 million or more in losses from a cyber attack.

The research shows that cyber risks rise dramatically as companies embrace new technologies, adopt open platforms, and tap ecosystems of partners and suppliers. While firms now report the biggest impacts from malware (81%), phishing (64%), and ransomware (63%), in two years they expect massive growth in attacks through partners, customers and vendors (247% growth); supply chains (+146%); denial of service (+144%); apps (+85%); and embedded systems (84%).

Surveyed companies see high risks from external threat actors, such as unsophisticated hackers (cited by 59% of firms), cyber criminals (57%), and social engineers (44%), but the greatest threat lies with untrained general staff (87%). Another 57% of firms see data sharing with partners and vendors as their main IT vulnerability. Nonetheless, only 17% of companies have made significant progress in training staff and partners on cybersecurity awareness.

“Companies need to make sure that their cybersecurity programs keep pace with their digital transformation efforts,” said Lou Celi, CEO of ESI ThoughtLab and director of the study. “Cybersecurity should not be an afterthought. It needs to be integrated into the fabric of an organization’s growth strategy.”

To win the arms race with hackers, companies are boosting their cybersecurity investments

To cope with rising cyber risks, surveyed companies are increasing their cybersecurity investment 7% this year and 14% next year. The biggest upsurge will come from platform companies, which are hiking their spending 59% this year and 64% next year. On average, companies with revenue between $250m-$1b will spend $2.9m next year; $1b- $5b ($5.7m); $5b-$20b ($10.7m); and $20b+ ($16.8m).

Next year, these firms plan to allocate 39.3% of their cybersecurity budgets to technology, 30.7% to process, and 30% to people. Companies now use a variety of technologies to improve cybersecurity, such as multi-factor authentication (90%), blockchain (68%), IoT (62%), and AI (44%). Over the next two years, they plan to

greatly expand their use of behavioral analytics (+1735%), smart grid technologies (+831%), deception technology (+684%), and hardware security and resilience (+114%).

Cybersecurity is still a work in progress

ESI ThoughtLab scored the surveyed companies based on their progress against each area of the NIST cybersecurity framework, then segmented these firms into three stages of cybersecurity maturity: beginners, intermediates, and leaders. The study's results reveal that companies have a long way to go with regard to cybersecurity maturity: only 20% of companies are leaders, while 31% are beginners and 49% are intermediates. Interestingly, technology firms have the lowest maturity scores — although platform companies have the highest. Financial services and insurance firms also tend to be further along the maturity curve than average.

According to the study, companies have made more progress on risk prevention than resilience. Over the next year, firms will continue to allocate the largest share of their investment to protection (26.5%), but will allocate more to respond (19.2%) and recover (18.1%) to increase resilience as attacks rise.

Cybersecurity maturity also varies by country: companies in the study with the highest maturity scores are based in the U.S. (107.2), South Korea (104.7), Japan (102.6), France (101.9), and Australia (101.3). Most of the lowest scoring companies were headquartered in emerging markets, including Brazil (88.6), Argentina (93.6), and India (93.7), although companies in Germany (97.3) and Switzerland (96.3) also had relatively low scores.

The returns on cybersecurity maturity

The study shows that as corporate cybersecurity systems mature, the probability of costly cyberattacks declines. Cybersecurity beginners have a 21.1% probability of cyberattacks generating over $1m in losses vs 16.1% for intermediates, and 15.6% for leaders. The costs of cyberattacks also decrease as cybersecurity matures: the costs for beginners is 0.039% of revenue ($3.9m for a $10b company) compared with 0.012% of revenue for leaders ($1.2m for a $10b company). However, these costs — and the number of successful attacks — are harder to measure for beginners due to their inadequate detection systems.

Despite better monitoring methods and metrics, most companies still do not know the ROI of their cybersecurity investments. One stumbling block is that firms often do not measure indirect costs, such as productivity loss, reputational damage, and opportunity costs, which can hurt bottom lines. Another is the difficulty of gauging risk probabilities and the failure to take into account the upside from improving productivity (cited by 35% of companies), profitability (22%), corporate reputations (18%), competitive positioning (16.2%), and customer engagement (11%).

"While cybersecurity will always be more of an art than a science," says Celi, "companies need to do a better job of measuring their full direct and indirect cost-benefits to understand where to invest to secure their digital future. This study is a major step in that direction."

About the research program

This pioneering research program, titled ***The Cybersecurity Imperative***, is based on a global survey of 1,300 organizations across industries and regions; research input from a high-level advisory panel; in-depth interviews with CISOs and leading experts; and rigorous benchmarking analysis. The research was conducted in the second quarter of 2018 in conjunction with a diverse coalition of sponsors, including Baker McKenzie, CyberCube, HP Inc., KnowBe4, Opus, Protiviti, Security Industry Association, and Willis Towers Watson.

For more information about the study and access to a complimentary thought leadership ebook, white paper, and cybersecurity benchmarking tool, please visit: www.esithoughtlab.com.

About our research team

ESI ThoughtLab: ESI ThoughtLab is the thought leadership arm of Econsult Solutions Inc., a leading economic consultancy. The innovative think tank offers fresh ideas and evidence-based analysis to help business and government leaders understand and respond to economic, industry and technological shifts around the world. Its team of top economists and thought leaders excel at creating valuable decision support that combines visionary thinking, analytical excellence, and multi-format content.

WSJ Pro Cybersecurity: WSJ Pro Cybersecurity is designed to help executives monitor the ever-changing landscape of cybersecurity through a business lens. Our dedicated team delivers unique, actionable insight on the wide-ranging challenges of cybercrime risk.

About our research sponsors

Baker McKenzie: Baker McKenzie helps clients overcome the challenges of competing in the global economy. We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

CyberCube: CyberCube delivers data-driven cyber analytics built specifically for the insurance industry. CyberCube is focused on solving the most difficult and important cyber risk challenges in insurance with world-class analytics. CyberCube offers a software-as-a-service platform for cyber risk aggregation modeling and insurance underwriting. The CyberCube platform was established in 2015 by Symantec and now operates as a standalone company with continued access to Symantec data and resources.

HP Inc.: HP Inc. creates technology that makes life better for everyone, everywhere. Through our portfolio of printers, PCs, mobile devices, solutions, and services, we engineer experiences that amaze. More information about HP Inc. is available at http://www.hp.com

Knowbe4: KnowBe4 is the world's largest security awareness training and simulated phishing platform that helps you manage the ongoing problem of social engineering. The KnowBe4 platform is user-friendly and intuitive. It was built to scale for busy security leaders and IT pros that have 16 other fires to put out. Our goal was to design the most powerful, cost effective and easy-to-use platform available.

Opus: Opus is a global risk and compliance SaaS and data solution provider founded on a simple premise: faster, better decisions in compliance and risk management give businesses an extraordinary advantage in the marketplace. Today, the world's most-respected global corporations rely on Opus to free their business from the complexity and uncertainty of managing customer, supplier and third-party risks. For more information about Opus, please visit www.opus.com.

Protiviti: Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Through its network of more than 80 offices in over 20 countries, Protiviti and its independently owned Member Firms provide clients with consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI), a member of the S&P 500 index. For more information, please visit www.protiviti.com.

Security Industry Association (SIA): The leading trade association for global security solution providers, the SIA brings together more than 850 member companies representing thousands of security leaders and experts who shape the future of the security industry. SIA protects and advances its members' interests by advocating pro-industry policies and legislation at the federal and state levels, creating open industry standards that enable integration, advancing industry professionalism through education and training, opening global market opportunities and collaborating with other like-minded organizations.

Willis Towers Watson: Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals.

###