ESI THOUGHTLAB **Driving Cybersecurity Performance**

Press Release

New report finds cybersecurity investment generates substantial ROI as large firms fend off rising cyberattacks

ESI ThoughtLab and group of cybersecurity advisors release findings from study of 1,009 of the world's largest firms.

June 18, 2020 (Philadelphia, PA). A comprehensive study conducted by ESI ThoughtLab reveals that increased investment in cybersecurity can generate a significant ROI of 179% and provide greater protection as companies cope with the fallout from COVID-19.

ESI ThoughtLab benchmarked the cybersecurity investments, practices, and performance metrics of 1,009 firms across 13 industries and 19 countries to identify the most effective approaches for mitigating cybersecurity risks and losses. This ground-breaking research was conducted in conjunction with an advisory group of cybersecurity, cyber insurance, and technology specialists, including Arceo.ai, Check Point Software, Cowbell Cyber, Edelman, Fiserv, KnowBe4, Optiv, and Verizon Business.

The analysis found that, last year, firms surveyed spent $9.6 million on average on cybersecurity ($515 per employee), and 97% of those expect to increase their spending by an average of 14% this year (pre-COVID-19 estimates). Companies are investing in three areas: people, process, and technology. While the average ROI is 179%, it ranges from 271% for investments in people, 156% for process, and 129% for technology. According to the research, on average, investments in people result in a 46% decline in the probability of a breach vs. 30% for process and 37% for technology.

"These cybersecurity investments can generate enormous ROI for companies, particularly for those in earlier stages of cybersecurity maturity," said Lou Celi, CEO of ESI ThoughtLab and the program director of the research. "The reliance on digital technology during the pandemic, together with the rise of remote working, shopping, and healthcare, have served as a stress test for corporate cybersecurity systems. Our CISO interviews have revealed that companies with advanced protection, detection, and response frameworks, backed up by strong cybersecurity hygiene and governance, have fared well during the crisis."

Companies still need to do more to combat rising threats

According to the surveyed companies, one in three attack attempts over the last year resulted in a successful breach. While most cybersecurity breaches are minor, affecting only a small number of people or machines, the average price tag per breach is around US$330,000. However, for firms that are in the top 10% in terms of breach costs, the average cost per breach is over $1.8 million. Adding to the complexity, companies may be underestimating their exposure to a potential breach and overestimating the protection offered by their cybersecurity systems. While the average company assigns a 45% probability to a moderate or material breach, the research shows that the probability is much higher, ranging from 62% to 86%.

The research shows that companies need to go well beyond compliance with cybersecurity frameworks, such as NIST or ISO, to be effective in reducing risks. For example, only 64 of 151 companies (42%) classified as leaders in NIST compliance are advanced in cybersecurity effectiveness, according to the study's rankings. Rather than applying the NIST framework as a box-ticking exercise, the most cyber-secure companies adapt this framework to their business goals, strategies, and individual risk profiles.

1435 Walnut Street, 4th Floor, Philadelphia, PA 19102
917-459-4614 Lceli@esithoughtlab.com esithoughtlab.com

Cybersecurity leaders also combine analysis from advanced quantitative tools and input from internal business partners and third-party experts to make the best decisions.

Even before COVID-19 hit, companies reported the largest losses from malware (66% of survey respondents), phishing (60%), and password reuse (49%), with cyber criminals cited as the biggest threat actors. As business goes digital over the next two years, executives also expect an increase in attacks through artificial intelligence (38%), denial of service (34%), and web applications (29%). With geopolitical and social unrest growing, and greater economic volatility ahead, CISOs in the financial, energy, automotive, retail, and telecom sectors are bracing for a jump in cyber terrorism and activism, along with greater risks from nation-states.

The most successful approaches of companies advanced in cybersecurity

The study identifies the practices of cybersecurity leaders that are most effective in mitigating cybersecurity risks and losses. Leaders commonly do six things that keep them well prepared for today's high-risk environment:

1. **Invest more in cybersecurity.** Leaders spend about 25% more than others on cybersecurity per employee, increase those investments each year more than the average, and invest more than others in recruiting specialists, working with external consultants, and training, such as end-user security awareness training with simulated phishing.
2. **Make cybersecurity hygiene a top priority.** Leaders have the lowest percentage of "critical" unpatched or "high" vulnerabilities based on CVSS scores (18% for leaders vs. 28% for others). They also do more frequent backup restoration drills (5.6 times a year vs. 4.3 for non-leaders), IT infrastructure scans (4.9 vs 3.4), and phishing tests (5.1 vs. 4.4).
3. **Keep management teams focused and aligned.** Cybersecurity heads typically report into the CEO, COO, or the Board in leader companies. CISOs at these firms focus more on security than IT (75% of leaders) and play a bigger role in managing data privacy (54%), digital transformation (57%), and operational resiliency (49%). Leaders are also more likely to make cybersecurity a shared responsibility of two executives, such as the CIO and CISO, or the CISO and CSO.
4. **Rely heavily on advanced analytics and specialized teams.** More than 8 out of 10 leaders conduct cyber-risk scenario analysis, assess the financial impact of risk events, and measure the effects of mechanisms to mitigate cyber risks. Leaders also outsource incident response, red team, risk management, and security ops more often than others.
5. **Extract greater value from cybersecurity tools.** Leaders invest more heavily in—and achieve greater effectiveness from—key cybersecurity technologies, including cloud workload security, endpoint detection, mobile device management, deception technology, email filtering, multi-factor authentication, and firewalls and web filtering.
6. **Make more use of cybersecurity insurance.** Since it is impossible to mitigate all risk, leaders rely more on insurance to transfer it: 57% of leaders have cyber insurance coverage over $10 million, compared with 30% of non-leaders. Overall, six out of 10 firms plan to spend more on cybersecurity insurance over the next two years.

"Companies across the board are improving their cybersecurity practices and reducing their losses thanks to smart investments in people, process, and technology," said Celi. "While these steps have helped contain cyberattacks during the pandemic, today's turbulent environment has underscored the value of business continuity and resilience, as well as using advanced analytics to assess cyber risks in an interconnected world."

The full findings of the study can be found at https://econsultsolutions.com/esi-thoughtlab/driving-cybersecurity-performance/

For media inquiries, please contact:

Lou Celi, Program Director
ESI ThoughtLab
917-459-4614
Lceli@esithoughtlab.com

Mike Daly, Marketing Director
ESI ThoughtLab
215-717-2777
Mdaly@esithoughtlab.com

About 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.

About Arceo.ai: Arceo.ai enables cyber resilience by combining smarter insurance products with dynamic security solutions. Headquartered in San Francisco, Arceo empowers insurers and brokers to better assess, underwrite, and manage cyber risks through a patented methodology called Cyber Meteorology. Arceo's holistic risk analytics and insurance platform enables enterprises to better identify, respond to, and recover from cyber risks using AI to drive advanced risk assessment and proactive security services. For more information, visit www.arceo.ai and stay up to date on our blog Twitter and LinkedIn.

About Cowbell™ Cyber: Cowbell Cyber maps insurable threats and risk exposures using artificial intelligence to determine the probability of threats and impact on coverage types. In its unique approach to risk selection and pricing, Cowbell compiles Cowbell Factors™, a set of risk-rating factors, that enable continuous underwriting and expedite quoting and binding for brokers. Cowbell Prime™, Cowbell's standalone, admitted, and individualized cyber coverage is available to small and mid-size businesses (SMBs) through a network of independent insurance agencies and brokers.

About Edelman: Edelman is a global communications firm that partners with businesses and organizations to evolve, promote and protect their brands and reputations. Our 6,000 people in more than 60 offices deliver communications strategies that give our clients the confidence to lead, act with certainty and earn the lasting trust of their stakeholders. We develop powerful ideas and tell magnetic stories that move at the speed of news, make an immediate impact, transform culture, and spark movements.

About Fiserv: Fiserv, Inc. (NASDAQ: FISV) aspires to move money and information in a way that moves the world. As a global leader in payments and financial technology, the company helps clients achieve best-in-class results through a commitment to innovation and excellence in areas including account processing and digital banking solutions; card issuer processing and network services; payments; e-commerce; merchant acquiring and processing; and the Clover® cloud-based point-of-sale solution. Fiserv is a member of the S&P 500® Index and the FORTUNE® 500 and is among FORTUNE World's Most Admired Companies®. Visit Fiserv.com and follow us on social media for more information and the latest company news.

About 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.

About Optiv Security: Optiv is a security solutions integrator – a "one-stop" trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, security operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler, more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com

About Verizon: Verizon Communications Inc. (NYSE, Nasdaq: VZ) was formed on June 30, 2000 and is celebrating its 20th year as one of the world's leading providers of technology, communications, information and entertainment products and services. Headquartered in New York City and with a presence around the world, Verizon generated revenues of $131.9 billion in 2019. The company offers voice, data and video services and solutions on its award-winning networks and platforms, delivering on customers' demand for mobility, reliable network connectivity, security, and control. Find out more about Verizon Business and read the 2020 Data Breach Investigations Report for in-depth analysis on the cyber trends impacting businesses.

###