ISF

World's Largest Cybersecurity Benchmarking Study Finds that Top Executives Believe their Organizations are Not Prepared for New Era of Risk

ThoughtLab – New York, May 10 2022

This landmark study provides private- and public-sector leaders with evidence-based insights into the cybersecurity practices and investments that are most effective for mitigating risks.

ThoughtLab, a leading global research firm, today announced the findings of its 2022 cybersecurity benchmarking study, ***Cybersecurity Solutions for a Riskier World.*** The study analyzed the cybersecurity strategies and results of 1,200 large organizations across 14 different sectors and 16 countries, representing $125.2 billion of annual cybersecurity spending.

The research revealed that the pandemic has brought cybersecurity to a critical inflection point. The number of material breaches respondents suffered rose 20.5% from 2020 to 2021, and cybersecurity budgets as a percentage of firms' total revenue jumped 51%, from 0.53% to 0.80%. During that time, cybersecurity became a strategic business imperative, requiring CEOs and their management teams to work together to meet the higher expectations of regulators, shareholders, and the board. In addition, the role of the chief information security officer (CISO) expanded, with many taking on responsibility for data security (49%), customer and insider fraud (44%), supply chain management (34%), enterprise and geopolitical risk management (30%), and digital transformation and business strategy (29%).

Yet 29% of CEOs and CISOs and 40% of chief security officers admit their organizations are unprepared for a rapidly changing threat landscape. The reasons cited include the complexity of supply chains (44%), the fast pace of digital innovation (41%), inadequate cybersecurity budgets and lack of executive support (both 28%), convergence of digital and physical assets (25%), and shortage of talent (24%). The highest percentages of unprepared organizations were in critical infrastructure industries: healthcare (35%), the public sector (34%), telecoms (31%), and aerospace and defense (31%).

Over the next two years, security executives expect an increase in attacks from social engineering and ransomware as nation-states and cybercriminals become more prolific. Executives anticipate that these attacks will target weak spots primarily caused by software misconfigurations (49%), human error (40%), poor maintenance (40%), and unknown assets (30%).

Ground-breaking analysis reveals industry metrics and best-performing cybersecurity strategies

As part of ThoughtLab's evidence-based research, its economists assessed the cybersecurity performance of corporate and government organizations against 26 metrics, including times to detect, respond to, and mitigate a cybersecurity breach, as well as the number of material breaches suffered. The benchmarking study revealed 10 best practices that can reduce the probability of a material breach and the time it takes to find and respond to those that happen:

1. **Take cybersecurity maturity to the highest level.** Organizations that are most advanced in applying the NIST cybersecurity framework outperform others on key metrics, such as time to detect a breach (119 days for advanced vs. 132 days for others). They also have fewer annual material breaches (0.76 for advanced vs. 0.81 for others).
2. **Ensure cybersecurity budgets are adequate.** ThoughtLab's analysis found a clear correlation between investment and results. Respondents reporting multiple material breaches in 2021 spent 12.3% of their total IT spending on cybersecurity, while those reporting no material breaches in 2021 spent an average of 12.8%, or $4.7 million more. Organizations that spent more also reported faster times to detect and mitigate a breach.

3. **Build a rigorous risk-based approach.** On average, risk-based leaders—i.e., those most advanced in quantitative analysis of risk probabilities and impacts—saw 22.5 incidents and 0.75 material breaches in 2021, vs. 27.1 incidents and 0.88 material breaches for risk-based beginners. In addition, 50% of top performers in time to mitigate took a risk-based approach vs. 17% of poor performers.
4. **Make cybersecurity people centric.** Cybersecurity is as much about humans as it is about technology. Organizations see fewer breaches and faster times to respond when they build a "human layer" of security, create a culture sensitive to cybersecurity risks, build more effective training programs, and develop clear processes for recruiting and retaining cyber staff.
5. **Secure the supply chain.** For 44% of respondents, the growing use of suppliers is exposing them to major cybersecurity risks. Top performers in time to detect, respond, and mitigate are far more mature in supply chain security. For example, over half of organizations with excellent times to detect are advanced in supply chain security vs. 25% of those with poor times to detect.
6. **Draw on latest technologies but avoid product proliferation**. Organizations with no breaches invest in a mix of solutions, from the fundamentals such as email security and identity management, to more specialized tools such as security information and event management systems (SIEMs). These organizations are also more likely to take a multi-layered, multi-vendor security approach to monitor and manage risks better through a strong infrastructure.
7. **Prioritize protection of links between information and operating technologies.** With digital and physical worlds converging, the attack surfaces for respondents are widening. Organizations that prioritize protection of interconnected IT and OT assets experience fewer material breaches and faster times to detect and respond.
8. **Harness intelligent automation**. Automation, combined with AI and orchestration, helps CISOs deliver results while freeing up staff from mundane tasks. For example, about three out of 10 organizations with excellent dwell times (the time to detect and remediate) use smart automation vs. 17% of organizations with poor dwell times.
9. **Improve security controls for expanded attack surfaces**. Attack surfaces widened during the pandemic because of greater digital transformation, cloud migration, remote working, and supply chain complexity. Our research shows that more companies need to put security controls in place to cover their expanding technology environments.
10. **Do more to measure performance**. Currently organizations track just 4.2 cybersecurity metrics on average. Executive teams that are more assiduous—monitoring six or more metrics—experience fewer incidents and material breaches. They also respond faster to attacks.

–

A coalition of cybersecurity experts from leading companies, associations, and universities

The research program drew on the expertise of a diverse group of cybersecurity leaders and experts from across the private sector, government, and academia. The group includes global consulting sponsor Booz Allen Hamilton; lead sponsors Elastic, KnowBe4, Skybox Security, Securonix, Claroty, Axis Communications, Votiro, and Zenkey; supporting sponsors ServiceNow, CyberCube, and Resolute Strategic Services; and research partners Internet Security Alliance and ISF. The advisory board consists of CISOs and other cybersecurity experts from a cross-section of industries.

"The move to digital during the pandemic—and now escalating geopolitical tensions—are ushering in a new era of cybersecurity risk that will require stronger leadership and wider teamwork among C-Suite executives and their staffs," said Lou Celi, CEO of ThoughtLab and the program's research director. "While there is no silver bullet, our evidence-based research reveals that organizations need to take their cybersecurity programs to a higher level of excellence by ensuring they are proactive, risk-based, human-centric, digitally advanced, and properly resourced."

"This landmark study fills a growing need for industry-specific cybersecurity metrics that companies can use to measure their performance against their peers," said Paul Sussman, vice president at Booz Allen Hamilton. "The research shows that firms have made considerable progress against cybersecurity frameworks like NIST, but they need to do more to keep their organizations safe."

A virtual panel discussion hosted by ThoughtLab and Resolute Strategic Services featuring Paul Sussman, Vice President, Cybersecurity Strategy Consulting, Booz Allen Hamilton; Duc Lai, CISO, University of Maryland Medical System; and Juan Morales, CISO, Realogy; will be held on Wednesday, May 25, 2022, from 11AM to noon EST to discuss the findings and key takeaways for public and private organizations. Register here.

The full report is available here: https://thoughtlabgroup.com/cyber-solutions-riskier-world/.

About ThoughtLab Group

ThoughtLab Group is an innovative thought leadership firm that generates business insights through rigorous research and economic analysis. We specialize in assessing the economic, financial, and social impact of latest technology on cities, companies, industries, and world markets. Our services include fielding business, consumer, investor, and government surveys; organizing executive interviews, meetings, and advisory groups; conducting economic modeling, AI sentiment monitoring, benchmarking, and performance analysis; and developing white papers, eBooks, infographics, and customer-facing analytical tools.

Additional commentary from sponsors

Steve Durbin, CEO, Information Security Forum: "The shift in landscape produced by the pandemic and cross-border conflicts has required organizations to reprioritize strategic objectives and key risks from accelerating digital transformation programs and migration to the cloud. CISOs must drive the conversation with the board, they must help address and answer difficult questions regarding cybersecurity and clarify misconceptions."

Stu Sjouwerman, CEO and President, KnowBe4: "The focus today is too much on trying to prevent data from leaving, instead of stopping attackers from ever getting in. I would expect to see more focus on security awareness training to reduce the threat surface of phishing—a primary attack vector in nearly every kind of cyberattack. This kind of training helps to establish good cyber hygiene, a sense of vigilance, and has been shown to reduce the risk of users falling for social engineering tactics employed within phishing attacks."

Augusto Barros, Vice President, Cybersecurity Evangelist, Securonix: "Organizations need to find the right balance between protective and reactive measures, such as detection and response. Security executives often invest more in protective measures and not enough to handle situations when they fail. These investments should allocate resources appropriately across people, process, and technology. Responding successfully to an attack is often human-driven, but it also requires effective processes and latest technologies, such as SOAR and EDR."

Wayne Dorris, Business Development Manager, Axis Communications: "Physical security devices like network cameras, AV systems, and access control devices are a blend of OT and IoT end points. Hardening these devices and managing vulnerabilities to the same requirements of your IT policies is often overlooked. Since most traditional IT security and cybersecurity teams do not have the knowledge or the tool sets to properly configure and manage these devices independently, it's important that they work closely with manufacturers that are leading in the space and can provide support."

Mandy Andress, CISO, Elastic: **"**The most prepared companies are the ones that have really focused on the fundamentals of good security hygiene: knowing your environment, updating and patching your technology, changing default configurations, and utilizing layers of security. Being solid on the basics closes most avenues that attackers leverage to access or move through an environment."

Gidi Cohen, CEO and Founder, Skybox Security: "A risk-based approach resulted in fewer breaches year over year. This fact underscores that proactive security posture management enables CISOs to act quickly and decisively to mitigate the risks with the greatest potential impact. Calculating true risk exposure requires understanding your entire attack surface with a network model. Then, comprehensive exposure management must combine threat intelligence, asset importance, path analysis, and attack simulation to pinpoint threats with the highest likelihood to impact your business financially."

Ravi Srinivasan, CEO, Votiro: "Most ransomware attacks happen when the bad actors have gotten your data and locked it up. So, the key thing is to follow the data. It's like they say with understanding political corruption: follow the money. If you want to understand ransomware, follow the data. You will find it moving from server to endpoint to the cloud to file shares—and that chain is what you want to protect. If you can protect that data chain before the bad actor is able to compromise it, you've successfully prevented ransomware."

Barbara Kay, Senior Director, Product Marketing for Risk, Security, and ESG, ServiceNow: "Risk-based management aligns security priorities with the business and helps security leaders become more strategic in their views. The board, business heads, CFOs, and CROs all think about risks and tradeoffs. Mature organizations work with IT and GRC teams to operationalize risk decisions within technical and process controls. The whole team goes faster, with less risk and friction, and more visibility."

Darren Thomson, Head of Cyber Intelligence Services, CyberCube: "As security and resilience become top of mind for corporate boards, the CISO needs to adapt culturally to demonstrate the impact of their efforts on the business. It is important for CISOs to talk to a board of directors in a language that they understand in order to take a strategic, top-down approach to risk management in cyber."

Simon Chassar, Chief Revenue Officer, Claroty: "As digital and physical assets continue to converge—particularly in industrial, healthcare, and other types of critical infrastructure environments—the only way to mitigate risk is to make hyperconnectivity more secure. Considering this, CISOs must ensure that their cybersecurity programs encompass all types of interconnected assets across the organization, whether they are IT, OT, or any other kind of internet-connected device in the Extended Internet of Things (XIoT)."

Research sponsors and advisors

Wayne Dorris, Business Development Manager- Cybersecurity, Axis Communications; Madeline Robson, Content and Communications Specialist, Axis Communications; Fredrik Larsson, Expert Security Architect, Axis Communications; Per Bjorkdahl, Director, Sustainable Sales Engagements, Axis Communications; Matt Feenan, Team Lead, Products and Solutions Marketing, Axis Communications; Paul Sussman, Vice President, Cybersecurity Strategy Consulting, Booz Allen Hamilton; Mark Taylor, Head of Commercial Strategic Alliances and Partnerships, Booz Allen Hamilton; Christopher Smith, Principal, Commercial Cyber Practice, Booz Allen Hamilton; Ken Yao, Senior Associate, Cyber Fusion Center, Booz Allen Hamilton; Simon Chassar, Chief Risk Officer, Claroty; Grant Geyer, Chief Product Officer and CISO, Claroty; Upa Campbell, Chief Marketing Officer, Claroty; Chelsea Sawicki, Senior Director of Product and Content Marketing, Claroty; Rebecca Bole, Head of Industry Engagement, CyberCube; Megan Radogna, Thought Leadership Content and Research Manager, Elastic; Riva Froymovich, Senior Director, Thought Leadership, Elastic; Joanna Huisman, Senior Vice President, Strategic Insights and Research, KnowBe4; Augusto Barros, Vice President and Cyber Security Evangelist, Securonix; Oliver Rochford, Senior Director, Security Evangelist, Securonix; Isabelle Coste, Senior Director, Demand Generation, Securonix; Sara Kingsley, Director of Product Marketing, Securonix; Raunika Nayyar, Manager, Marketing and Communications, Securonix; Richard Murphy, Editor in Chief, Director, C-Suite Communications, ServiceNow; Barbara Kay, Senior Director, Product Marketing for Risk, Security, and ESG, ServiceNow; Kathy O'Connell, Vice President, Corporate Marketing and Communications, Skybox Security; Ashley Nakano, Corporate Communications Director, Skybox Security; Rob Rosiello, Chief Revenue Officer, Skybox Security; Kristin Melville, Vice President of Growth Marketing, Skybox Security; Ravi Srinivasan, CEO, Votiro; Gianna Whitver, Vice President of Marketing, Votiro; Alex Schlager, Chief Executive Officer, ZenKey; Larry Clinton, President/CEO, Internet Security Alliance; Jeff Brown, Former VP and CISO, Raytheon; Gary McAlum, Board Director, National Cybersecurity Center; Ron Mehring, CISO, Texas Health Resources; Peter Keenan, CISO, Lazard; Andrew Jenkinson, Group CEO, Cybersec Innovation Partners; Juan Morales, CISO, Global Information Security,Realogy Holdings; Dr. Ivo Pezzuto, Core Professor of Digital Transformation, Disruptive Innovation,International School of Management; Richard Rushing, CISO, Motorola Mobility, a Lenovo company; Dave Estlick, CISO, Chipotle Mexican Grill; Ilan Abadi, Global CISO, Teva Pharmaceuticals; Deborah Wheeler, SVP, Chief Information Security Officer, Delta Air Lines; Joseph Steinberg, Cybersecurity Expert Witness and Advisor, Cybersecurity and Artificial Intelligence Expert Services; Steve Durbin, CEO, Information Security Forum; June Chambers, Head of PR and Corporate Communications, Information Security Forum; Matthew Saidel, Vice President, Resolute Strategic Services; Curley Henry, Vice President, Deputy CISO, Southern Company; Mandy Andress, CISO, Elastic; Alim Somani, Managing Director, Hatch Digital