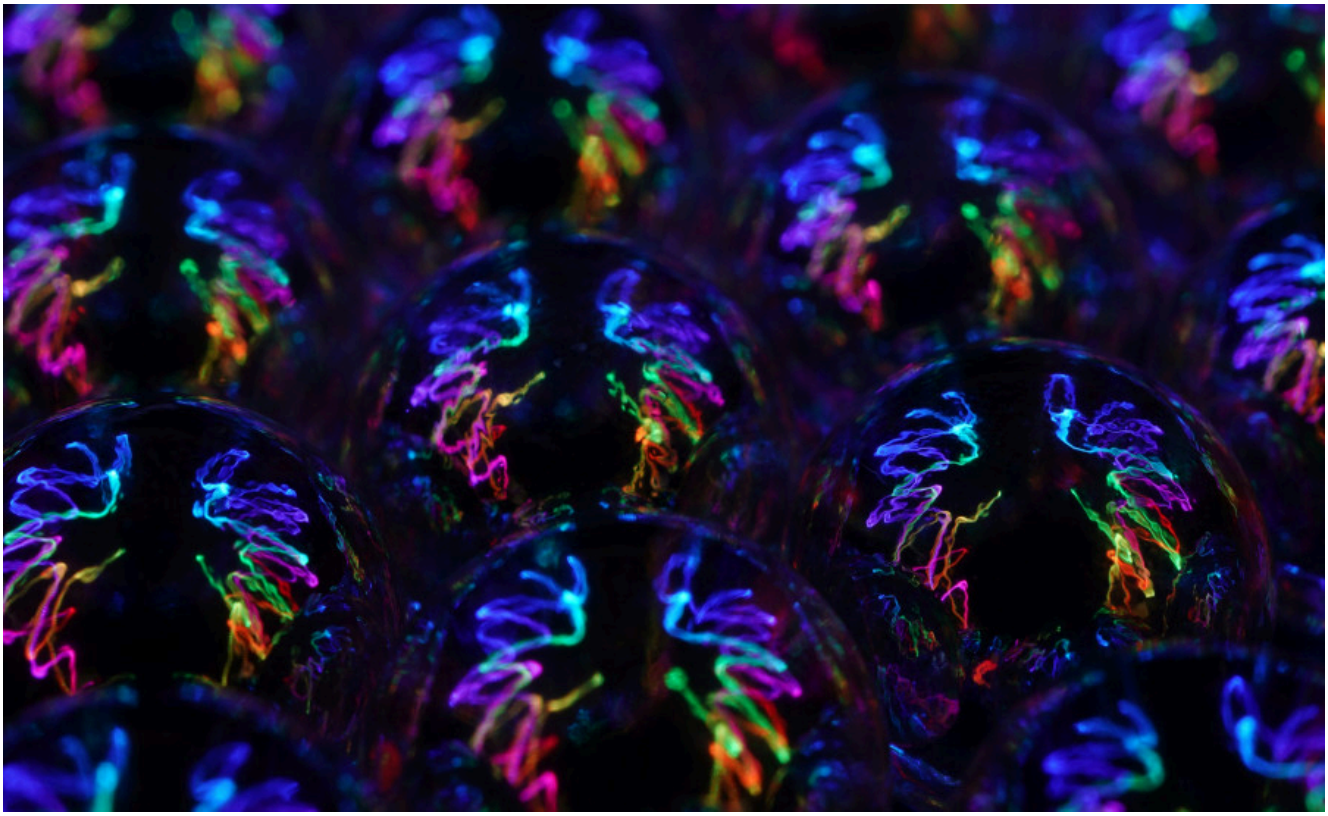
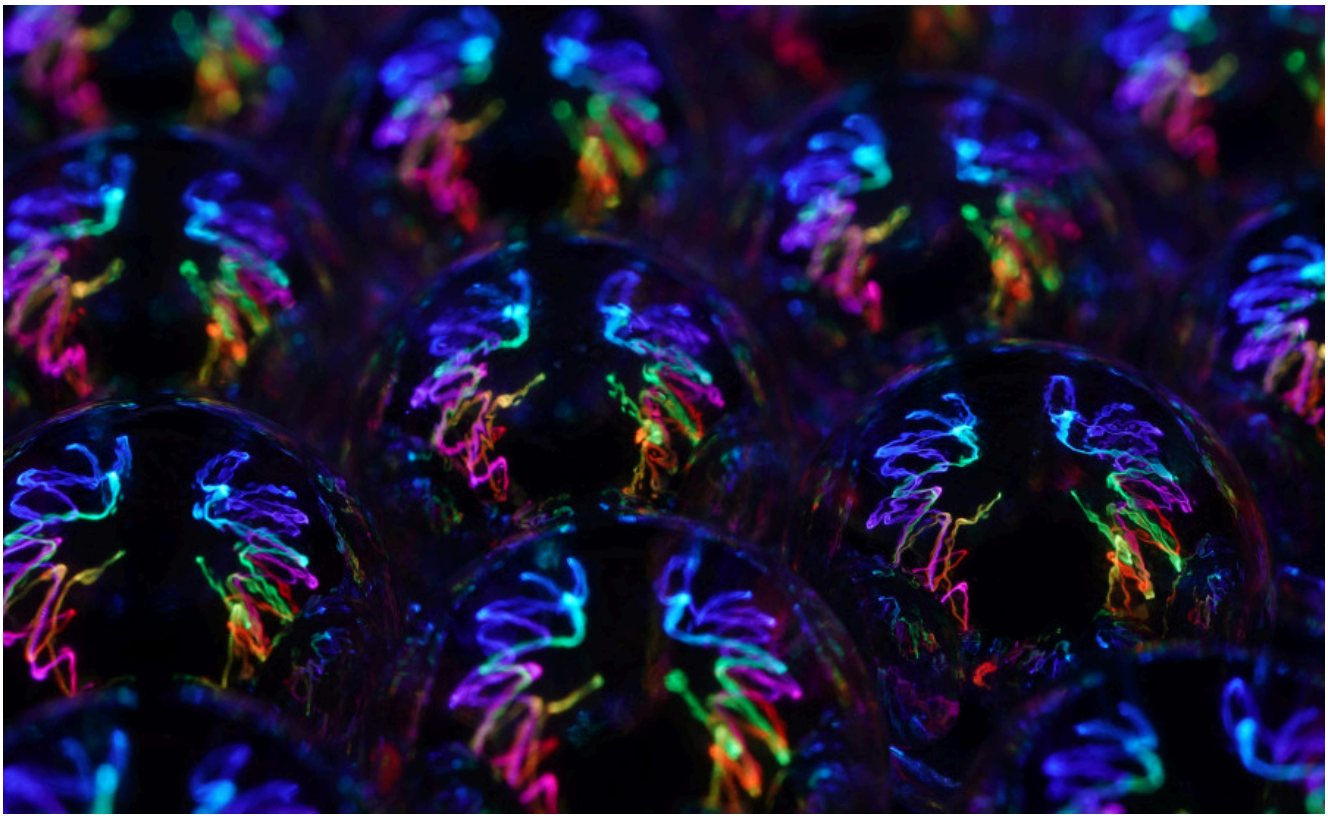
Knowledge is key to mitigate risk, maximize resilience





Constantly looming on the horizon, the pervasive threat of

physical and cyberattacks is always top of mind for security leaders. It is imperative for security leaders to educate themselves and remain vigilant and aware to ensure resilience in the ever-evolving threat landscape.

According to a recent report, cyber incidents such as ransomware, data breaches and IT disruptions are the top concern of 2024 with cyber replacing business interruption as the leading risk. According to the report, the resilience gap between large and smaller companies is widening, as risk awareness among larger organizations has grown since the pandemic with a drive to upgrade resilience. The report highlights that smaller businesses “often lack the time and resources to identify and effectively prepare for a wider range of risk scenarios and, as a result, take longer to get the business back up and running after an unexpected incident.”

The report also revealed that key risk management priorities in 2024 continue to be improving business continuity management, identifying supply chain bottlenecks and developing alternative suppliers.

As cyberattacks continue to increase in both amount and sophistication, it is vital for security leaders to protect digital identities within an organization ensuring only the correct people have access to the right data, network and systems.

According to the Identity Defined Security Alliance (IDSA) 2023 Trends in Identity Security report, 90% of organizations reported at least one identity-related incident in the last 12 months, a 6% increase from last year’s report. The report also revealed identity stakeholders are facing an increasing number of barriers without the support from leadership with 49% reporting their leadership teams understand identity and security risks and proactively invest in protection before suffering an incident, while 29% only engage and support after

an incident.

A report released in December highlighted the importance of critical infrastructure cybersecurity. The report found that 90% of the world's leading energy companies experienced a third-party data breach in the past 12 months while 100% of the top 10 U.S. energy companies experienced a third-party breach.

The report also revealed that 92% of the energy companies evaluated had been exposed to a fourth-party breach. The MOVEit vulnerability, revealed in June of last year, was a widespread third-party vulnerability in the last six months which impacted hundreds of companies and organizations around the world.

As part of Critical Infrastructure Security and Resilience Month in November, the Cybersecurity and Infrastructure Security Agency (CISA) highlighted some best practices critical infrastructure organizations could implement in order to recover quickly from a significant disruption. These best practices included:

- **Assess the risk –** Organizations should identify their most critical functions and assets, define dependencies that enable the continuity of these functions and consider the full range of threats that could undermine functional continuity.
- **Make a plan and exercise it –** Organizations should perform dedicated resilience planning, determine the maximum downtime acceptable for customers, develop recovery plans to regain functional capabilities within the maximum downtime and test those plans under real-life conditions to ensure the ability to operate through disruption.
- **Continuously improve and adapt –** Organizations should be prepared to regularly adapt to changing conditions and threats. This starts with fostering a culture of

continuous improvement, based on lessons learned from exercises and real-world incidents and evolving cross-sector risks.

Being aware of current cyber threats and staying educated on the latest trends are important tools in any security leader’s tool belt to help mitigate risk and improve resilience in today’s ever-evolving threat landscape.

https://www.securitymagazine.com/articles/100371-knowledge-is-key-to-mitigate-risk-maximize-resilience