# Cybersecurity: A Growing Need for all Businesses

*Malk Insights — April 2024*

## Key Takeaways

- Cyberattacks pose material threats to most companies regardless of size and industry and can have far reaching impacts beyond business operational disruptions. A key example of related consequences can be seen in the outcome of a recent cyber-attack on Change Healthcare, a breach that impacted the ability for providers across large and small healthcare systems to process payments, leading to patients receiving delayed care and medication.
- Cyberattacks are only expected to increase, with the U.S. government specifically focused on potential attacks on infrastructure (e.g., utilities, transportation) systems. This risk further highlights the need for cyber security enhancements for businesses that might not necessarily collect personal data and as such may not consider such controls in the normal course of business.
- Cyberattacks are costly, and smaller businesses, which are often victims of such attacks given reduced investment in privacy and security controls, may not be able to recover financially from a significant breach.
- Investors can take active steps towards mitigating cyber risks across their investments; businesses of all sizes should focus on building the foundations of a strong cybersecurity program to mitigate risk reduce the cost and business disruption of an incident and attract investors.

## The need for cybersecurity

Technology has become a ubiquitous need for businesses across all industries, including those that are not historically tech-advanced or even tech-reliant. As companies increasingly digitize their operations to keep up with shifting technology headwinds and gain an edge over competitors, the greater the potential opportunities for bad actors to exploit unprotected systems. Such risk is especially pertinent for companies and industries with historically limited uses for technology as they may not understand the need for cyber security or have strong controls in place.

Cyberattacks have been on the rise due to tailwinds such as the widespread adoption of remote work and virtualized IT environments (e.g., infrastructure, cloud computing), and are expected to continue growing. Outside of privacy concerns related to potential breaches of sensitive information, cyberattacks are incredibly costly to businesses—the global cost of cybercrime is expected to increase significantly over the next four years, from $9.22T in 2024 to nearly $14T in 2028. In fact, over 80% of businesses have experienced a cyberattack or data breach. As such, both asset managers and companies alike must understand and operationalize the business case for strong data security practices, as an upfront investment in data security programming can offset more significant losses down the road.

## Cost of an attack

The global average cost of a data breach in 2023 was $4.45M, representing a 15% increase since 2020. The hefty price tags businesses must pay are a result of an accumulation of theft of intellectual property, business disruptions, and costs associated with remediation or the recovery of data, including fines, penalties, and lawsuits. Further, cyberattacks on businesses that operate, invest in, or manage critical infrastructure, such as power grids, utilities, transportation systems, or healthcare systems can endanger public safety in addition to resulting in significant financial losses.

On February 21st 2024, for example, a cyberattack on the largest healthcare payment company, Change Healthcare, which was formerly private equity backed, caused hundreds of providers, ranging from large hospital systems to single-doctor practices, to lose the ability to obtain insurance approval or be paid for necessary services such as prescriptions and medically necessary surgeries. As Change Healthcare handles over 15 billion transactions annually, the 25-day blackout left millions of providers and patients with reduced or no access to care, prompting meetings with the White House and an investigation by the Department of Health and Human Services (HHS).

Additionally, a recent report to U.S. governors from the Biden Administration and the Environmental Protection Agency (EPA) alerted states to potential cyber-attacks on water and wastewater systems, which are critical to their communities' infrastructure. The lack of cybersecurity protections common to older infrastructure systems, along with the large amounts of people that would be impacted by a breach or ransom makes them attractive targets for attackers who are largely motivated by financial gain and incentivize payouts by creating disruption. The impacts of such a breach would be far ranging, pausing not just business operations but community and potentially state processes, exemplifying the need for cybersecurity controls regardless of a company's industry or data collection/processing practices.

While cyber incidents involving large businesses may result in widespread harm, small businesses are also vulnerable to malware, ransomware, and other attacks. The difference is that small companies may not survive such an incident. In fact, not only did 53% of small businesses (companies with 1,000 or less employees) fall victim to cyber-attack in 2023 — likely because small business often lack robust cybersecurity programming — but 60% of small businesses that suffered a cyberattack went out of business within six months. Responding to a cyber attack is costly and time consuming for small business who, in addition to paying ransoms, may face customer lawsuits and data privacy regulatory penalties. Ransomware attacks are increasingly impacting these businesses, with recent research noting that in 2023, small businesses paid a median of $16,000 to bad actors holding data hostage, with only 50% of those that paid the ransom receiving complete restoration of seized data. While data shows an increase in IT security spending and cyber insurance, there are various practices that all companies can implement, regardless of size or industry, that may greatly reduce risk of a cyber security incident.

## How to Prepare

Companies, regardless of size, should enhance their data privacy and security programs to include prevention practices. Such efforts include maintaining an up-to-date information security policy, providing employees with annual trainings inclusive of phishing simulations – the most common attack vector – and performing regular system vulnerability tests. These practices can reduce the risk of an incident by preparing employees and identifying potential attack vectors in a timely manner. Additionally, strong cybersecurity controls can distinguish companies – especially those in industries not typically associated with technology – from peers and

attract investors. Certifications such as ISO 27001, SOC 1, and SOC 2 certifications can also signal robust cybersecurity controls to investors. As certificantion achievement may be costly and resource intensive, making them challenging for small and growing businesses to achieve, investors can seek companies with cybersecurity programming aligned with key frameworks (e.g., NIST, CIS) and certification requirements. Upon investment, investors can assist portfolio companies in conducting cybersecurity risk assessments, gaining insight into programmatic gaps and visibility into any costs associated with remediating high priority or critical findings.

Investors should be cognizant of cybersecurity risk when performing diligence on investments or acquisitions and should include cyber considerations in post investment roadmaps. As shown by Change Healthcare, a formerly Private Equity backed company, investor emphasis on data privacy and security maturity may prevent debilitating incidents during and after the hold period. Strong cybersecurity practices do not necessarily require large budgets, and investors can implement foundational practices tailored to company cost and personnel constraints. There may also be additional cybersecurity risks specific to a company's operations that require bespoke controls (e.g., generative AI policy, open-source code reviews) that Malk is well positioned to assist clients and portfolio companies in identifying and developing.


**Authors**

**Alana miro**
*Senior Associate*
**e:** amiro@malk.com

**Christina Tedeschi**
*Engagement Manager*
**e:** ctedeschi@malk.com

**Rae Edmunds**
*Senior Associate*
**e:** redmunds@malk.com




## About Malk Partners

Malk Partners is the preeminent advisor to private market investors for creating and protecting value through environmental, social, and governance ("ESG") management and impact investing. Founded in 2009, Malk Partners advises many of the world's leading alternatives managers investing across private equity, growth equity, venture capital, and private credit by helping them define ESG goals, achieve ESG results, and guide their portfolio companies in driving value creation and mitigating risks. The firm is headquartered in La Jolla, California with an office located in New York. For more information about Malk Partners, please visit www.malk.com.