



Entering the New Era of Risk and Compliance

Organizations now rapidly adopt advanced technologies and methodologies to meet changing customer demands, reduce operational costs and comply with increased regulations without creating new risks and regulatory complications. Risk management teams stand ready to develop entirely new approaches to uncertain risk environments. But first, business leaders must identify the most imperative threats in the industry to invest in the right technologies, resources and workforce skills.

What You Will Find Here

- 01** Introduction
- 04** A look back: the risk and compliance landscape in 2021
- 05** The cost of non-compliance
- 07** A look forward: top risk and compliance trends to watch
- 14** What will the future of risk and compliance look like?



Professionals the world over are preparing for a new era of risk. Environmental, social and governance (ESG) concerns, heightened third-party risk, surging fraud and cybercrime, and high-stakes terrorist financing threats define the modern-day cyberthreat landscape. All this, in addition to an unpredictable pandemic, rapid digital transformation and a turbulent geopolitical market have taught executives to expect the unexpected.

In 2022, risk and compliance teams recognize the need to build proactive business and technology processes and platforms capable of detecting threats and mitigating risk before it's too late.

Our top risk and compliance trends forecast will help executives, CISOs and risk managers invest in the right technologies, appropriately train and mandate their teams, and respond faster to today's most significant challenges.

A look back: the risk and compliance landscape in 2021

Our 2021 Global Threat Intelligence Report identified the major threats organizations faced globally throughout the last year.¹ The survey includes 1,350 online interviews with technology and business decision-makers in large organizations across 15 industry sectors about the importance of key business and security issues relevant to secure operations.

The report highlights several events that transformed the risk and compliance landscape and influenced how leaders across industries responded. Notable changes in the landscape include the following:

- 62% of all attacks targeted the finance, manufacturing, hospitality and healthcare industries
- Miners and trojans replaced spyware as the most common malware family globally
- Coin miners accounted for 41% of all detected malware
- COVID-19 heightened advanced persistent threat (APT) groups
- Work-from-home and remote access magnified web and application attacks; 67% of all attacks were remote access on web applications (32%) or application-specific (35%)
- Privacy and protection became part of the new normal as new laws and regulations increased obligations, restrictions or limitations on the ability to transfer personal data to other countries



The cost of non-compliance

Organizations that fail to comply with new regulatory requirements and mandates pay more than just a dollar value. Depending on the extent of non-compliance, organizations that violate regulations are subject to the following unintended consequences:

- **Business disruption** with the slow or halt of routine business activities due to non-compliance consequences or legal complications
- **Productivity loss** with an overall decline making ripple effects on the ability to hit annual objectives
- **Revenue loss** due to business disruption and productivity loss
- **Customer loss** with dwindling customer trust and loyalty, especially when non-compliance (for example, a data breach) directly impacts customers
- **Fines, penalties and settlement costs** imposed by regulatory organizations
- **Reputational damage** as the long-term damaging effects of negative media attention impact brand image and customer confidence

Loss of institutional value based on lower safety and soundness solvency ratings from regulatory agencies. Recent years have seen organizations across all industries subjected to astronomical fines, including financial institutions, financial technology companies, airlines and ride-sharing service providers. In many cases, companies that fail to admit non-compliance and attempt to conceal data breaches or cyberattacks face even harsher consequences from regulatory enforcers.

The following case studies represent a few of the most expensive instances of non-compliance:

- In 2017, Equifax left a critical vulnerability unpatched for months, compromising the financial and personal information of more than 150 million people. This instance of non-compliance resulted in a \$1.4 billion settlement (not including legal fees), making it the most expensive example of non-compliance.²
- In 2018, British Airways failed to comply with the General Data Protection Regulation and suffered a

card-skimming attack that harvested the payment and personal data of more than 500,000 customers. The UK's Information Commissioner's Office fined the airline an unprecedented \$230 million.³

- In 2016, Uber Technologies came under fire when a cybercriminal breached the data of 57 million user accounts and 600,000 drivers, and the company paid the criminal \$100,000 to keep the breach quiet. The company faced a \$148 million fine, the largest ever issued for a data breach at the time.⁴

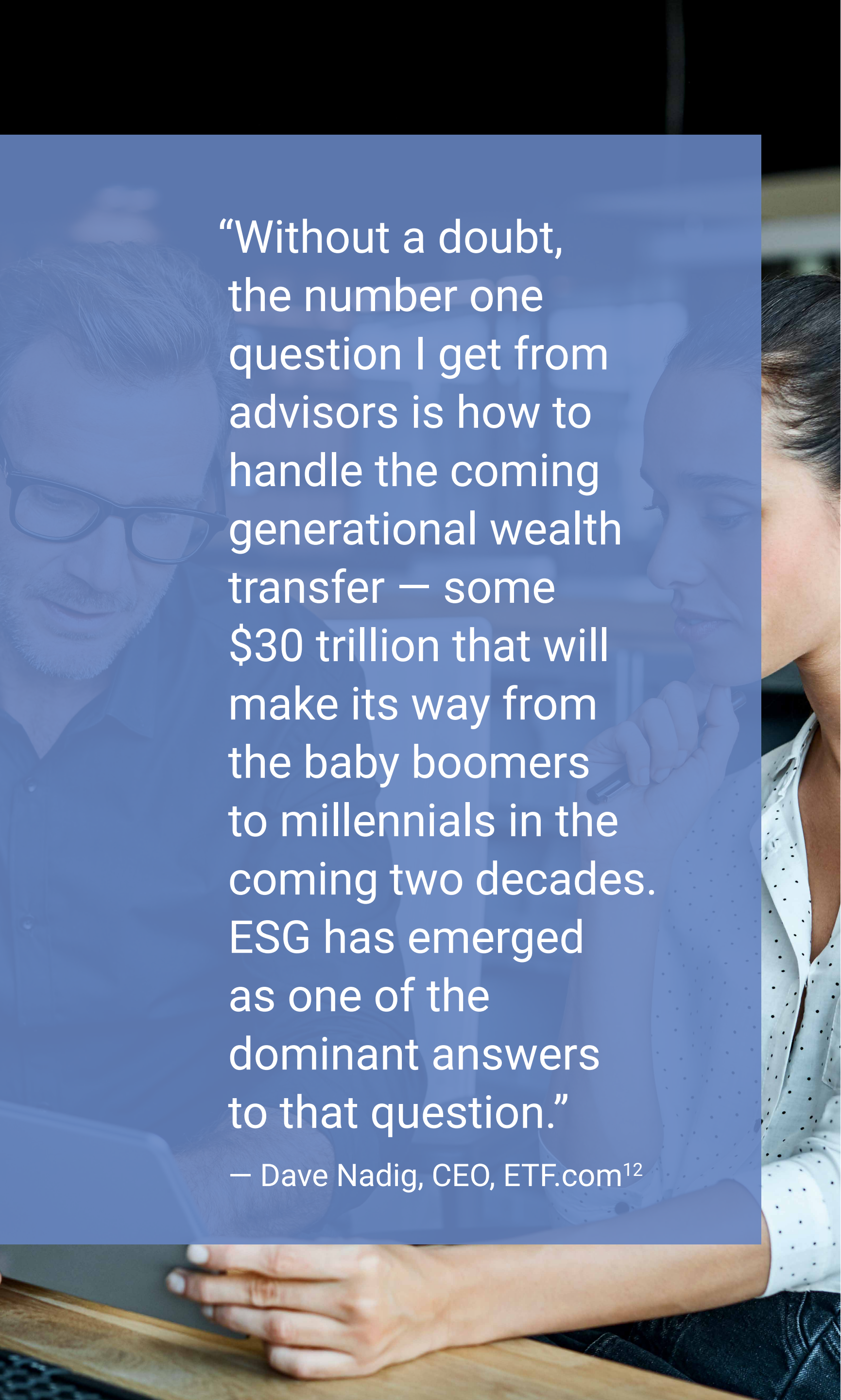
Overall, studies show the cost of non-compliance is 2.71 times higher than the cost of compliance and can range from \$14 million to \$40 million.⁵ However, as the cases described above show, with the combination of business disruption, productivity loss, revenue loss and high fines, costs can amount to even more.



Monitoring and sustainability are two heightened expectations from the regulators today. Are you monitoring your business to ensure that your journey to the digital delivery channels is not causing harm or unintended consequences? Can you react fast enough to mitigate that risk and change course correction before it catches the attention of the regulators or damages your customer base?

— Edmund Tribue, Vice President,
Leader of Risk & Compliance
Practice, NTT DATA⁶



A man with glasses and a woman are looking at a laptop screen. The man is on the left, wearing glasses and a dark shirt. The woman is on the right, wearing a white polka-dot shirt. They are both looking down at the laptop, which is on a wooden desk. The background is blurred.

“Without a doubt, the number one question I get from advisors is how to handle the coming generational wealth transfer — some \$30 trillion that will make its way from the baby boomers to millennials in the coming two decades. ESG has emerged as one of the dominant answers to that question.”

— Dave Nadig, CEO, ETF.com¹²

A look forward: top risk and compliance trends to watch

Risk management teams confront uncertainty every day. Over the last several years, leaders have faced a high level of uncertainty, including a pandemic, complications within third-party partnerships, geopolitical pressures, ESG demands, and volatile crypto and online risks.

Although we can't predict what the future holds for risk managers, five prominent risk and compliance trends will redefine how leaders conduct business. We believe it's paramount that organizations consider these trends in their strategy, technology and business processes to mitigate risk and meet evolving regulations in the coming years.

1. The importance of sustainability, environmental impact and compliance

Organizations hyper-focus on environmental impact and must comply with ESG obligations to mitigate reputational risks. Companies use ESG standards to screen operations and investments and ensure these practices are socially conscious.⁷

Non-ESG investments pose significant risks and regulatory complications for organizations. Sometimes known as sin stocks, these investments are associated with unethical activities that exploit human flaws. Oil companies, tobacco companies, alcohol companies and weapon manufacturers are considered sin stocks.⁸ The disadvantages of non-ESG practices and investing include:⁹

- Greater political risk
- Greater risk of declaring bankruptcy
- Greater reputational risk
- Higher taxes
- Negatively impacting the environment and the community

ESG criteria help organizations avoid partnering with and investing in high-risk companies that engage in unsustainable or harmful practices. At a minimum, organizations and investors must understand how climate change will affect their investments and intentionally invest in the transition to a low-carbon economy.

Many innovative, value-driven companies are already making changes. Microsoft, for example, announced a commitment to be 100% carbon-negative in the next 10 years and eliminate its past carbon emissions by 2050. The company also launched a \$1 billion fund for climate innovation.¹⁰

Ethical practices pay off. Millennials represent 79.4 million individuals in the United States, and there's currently a \$30 trillion intergenerational wealth transfer occurring from baby boomers to their millennial children.¹¹

In a typical intergenerational shift, firms lose approximately 70%–80% of assets. Among high net worth millennials, 95% are interested in sustainable investing. Companies that commit to ESG are well positioned to attract and retain investors, improve financial outcomes and mitigate risks.¹¹

2. The pace of digital transformation accelerating regulatory changes

Companies face unexpected consequences and disruptions as they scale digital transformation efforts. Although accelerated transformation triggers digital risks, the most significant threat to organizations is continuing to use outdated legacy systems and failing to adapt to new digital demands and regulations.

The new era of risk and compliance will see digitized compliance programs capable of handling technological acceleration and disruption. These programs help organizations automate regulatory requirements and reduce the cost of compliance.

Risk managers and organizational leaders leverage robust and interconnected ecosystems to automatically monitor risk and compliance activity. For example, trade surveillance and market risk tools help organizations oversee digital asset exchange in the crypto trading space. Advanced technologies enable leaders to monitor trading, operations, risk management and compliance across multiple asset classes.¹³

How can organizations continue to accelerate digital transformation while minimizing unintended risk? Proactive leaders in the risk space are transitioning from weak manual controls to intelligent automated interfaces to upgrade operating systems and processes. The most harmful cyberattacks often target technology gaps and outdated systems. Although it may never feel like the right time to phase out old systems, cybercrime is more costly and inconvenient than digital transformation.



“

It's akin to changing the tires on a racing car while it's lapping at speed. We cannot shut down the bank for six, nine, 12 months as we prototype some of these capabilities. We've got to be able to get them available — be ready, be nimble, be complex — without being complicated.

— Gordon Cameron,
Chief Consumer Credit Risk Officer,
Fifth Third Bank⁶

”

“This is a new era of business negotiation. It's just the way you're going to have to negotiate and think about creating partnerships and relationships in the future. And that includes aggregators who are using permission data and using standardized, secure APIs.”

— Chris Acevedo, Managing Director, Financial Services Consulting, NTT DATA⁶

3. The focus on third-party risk management

Many organizations outsource tasks to third-party vendors and subsequently increase exposure to unpredictable risks. Risk leaders must focus on vetting, tracking and managing third-party compliance, and organizations shouldn't allow unvetted access to data or assign blind trust to new alliances, partners or vendors.

Risk management and fraud management aren't static processes — both evolve constantly alongside new tactics, increasingly intelligent fraudsters and volatile markets. The ideal third-party partner must demonstrate the ability to change with the trends.

In December 2021, the U.S. Department of Justice and the Securities and Exchange Commission issued a warning about the importance of third-party risk management through due diligence questionnaires and compliance certifications, two risk management tools that have become prevalent since the Foreign Corrupt Practices Act (FCPA).^{14,15}

Organizations must vet third-party partners to mitigate fraud. It's essential to ask the following questions when evaluating risk and the compatibility of a partner:

- Will they share confidential information, customer data or sensitive personal data with third parties? This will help you understand the organization's third-party relationships.
- Does the third party abide by new regulations or display a history of non-compliance? This will help ensure contracts align and comply with new laws.

- Have they implemented and tested available third-party risk management and due diligence software? It's important to employ third-party risk management processes to detect and mitigate risk.
- How often will you conduct audits of third-party partnerships? By regularly auditing third-party partners, you can assess whether they continue to meet the terms and conditions of your original contracts.
- What procedures do they have in place to address fraud, account breaches, and other cybercrime and non-compliance?

Choosing the right providers, partners and vendors can help avoid serious risk to the business. As a result, more leaders are investing in third-party trust management (TPTM) platforms that evaluate third-party partnerships across core domains like security and privacy, ethics and compliance, and ESG.

TPTM includes third-party risk management software, third-party due diligence software, and supplier sustainability and responsibility to flag each type of risk. Ideally, TPTM should be centralized and operate under a singular workflow so teams can easily access and monitor risks as they come up.



Our 2021 Global Threat Intelligence Report shows that executives' top three cybersecurity focus areas in the next 18 months include:

50%

Cloud services

49%

Protecting the network

49%

Security data and applications

4. The rising risk of data breaches

Data protection is top-of-mind for organizational leaders in a digital-first environment. As a result, leaders spend more on cybersecurity and privacy initiatives to protect customer data, assets and reputations.

The U.S. State Department's recently announced Rewards for Justice program seeks to obtain information on foreign malicious cyberactivity against the United States. The program offers bounties of up to \$10 million for evidence leading to the identification or location of criminals participating in ransomware attacks against critical U.S. infrastructure at the direction or under the control of a foreign government.¹⁶

In addition, companies have seen an unprecedented number of cybersecurity compromises, data breaches and even demands for crypto ransoms. Some of the largest data breaches in history occurred in 2021, including the following:

- Hackers identified a gap in Facebook's security and posted 533 million user records from 106 countries on a hacking forum.¹⁷
- Unauthorized parties accessed 500 million records containing sensitive customer information, trade secrets and other intellectual property from the telecommunications company Syniverse.¹⁸
- An unprotected database exposed more than 13 million records from Amazon vendors and released email addresses, WhatsApp phone numbers, PayPal account details and more.¹⁹
- Over a thousand misconfigured Power Apps from Microsoft accidentally exposed 38 million records to the public and leaked people's COVID-19 vaccination status and personal data, including home addresses and phone numbers.²⁰

Our 2021 Global Threat Intelligence Report shows that executives' top three cybersecurity focus areas in the next 18 months include protecting cloud services (50%), protecting the network (49%), and securing data and applications (49%).¹ All these areas are essential in the mission to protect sensitive organizational and customer data.



As a compliance professional, I do not see the regulatory oversight being more permissive for unsecured data or unsecured data practices due to the pandemic. There are inherent vulnerabilities with thousands of people working from their homes with no substantive physical oversight. Insurance organizations should expect further change, whether from an operating model standpoint or regulatory oversight, and they must remain flexible with their dynamic workforce.

— Bill Sun, Director of Compliance and Internal Controls, NTT DATA²¹



5. The need for employee awareness and compliance training

Organizations equipped with the best cybersecurity and privacy settings are still vulnerable to internal risk via unaware employees. As a result, risk and compliance training will continue to expand to teach employees how to avoid phishing scams, data breaches, account takeovers and more.

COVID-19 required organizations to embrace remote work environments while confronting a new level of digital operations and the new risks associated with these changes. Agencies that govern compliance requirements will continue to strengthen regulations around data security and consumer privacy.

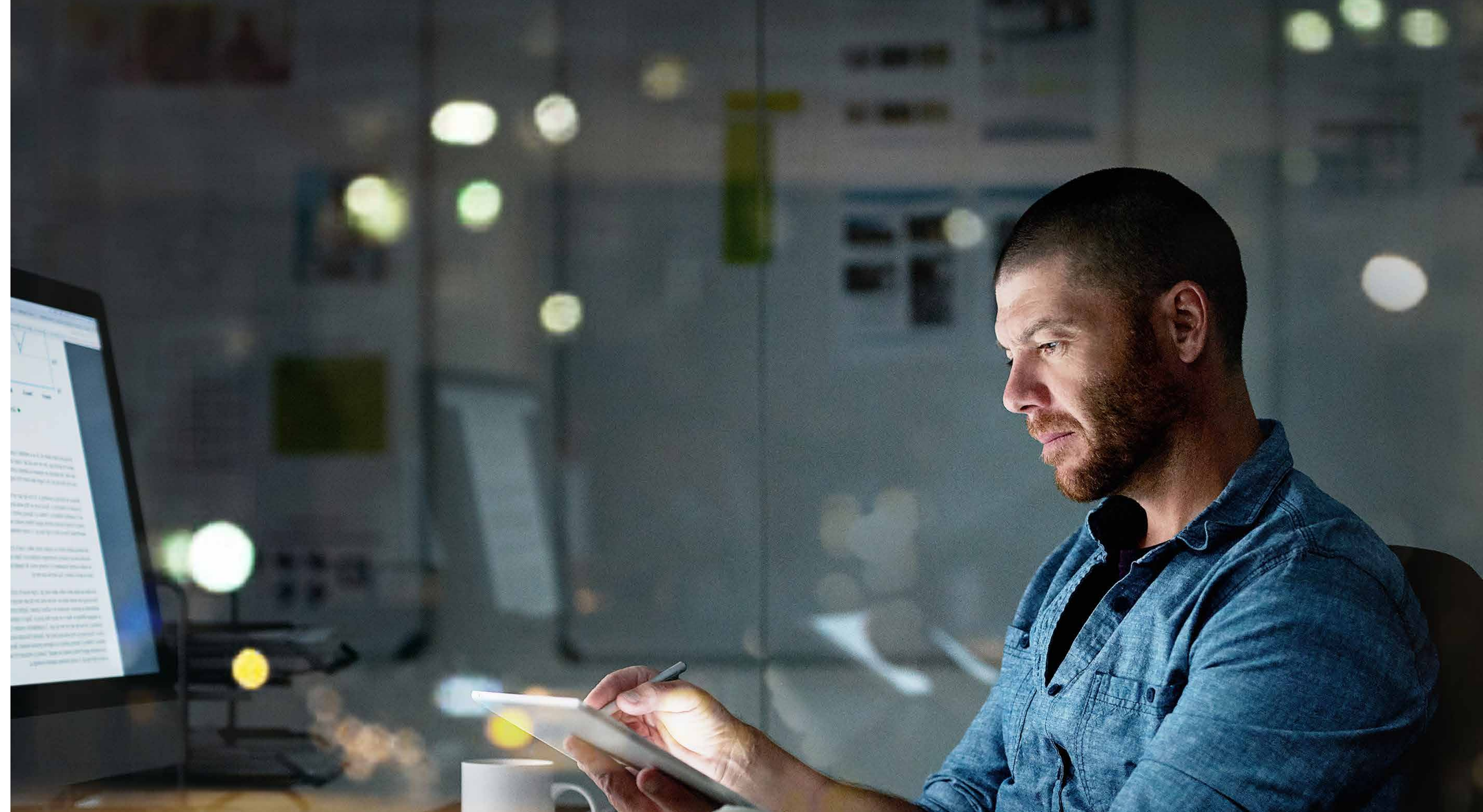
First, organizations should review and update existing data security and privacy training programs geared toward traditional brick-and-mortar buildings to account for a remote workforce. Next, leaders must retrain teams on security best practices in a remote setting.

Leaders must implement new approaches to manage risk, achieve process standardization, establish ownership and governance, and empower teams to understand and apply lessons from compliance training.



What will the future of risk and compliance look like?

- As digital transformation accelerates and the geopolitical and environmental climates continue to evolve, the state of risk and compliance will be in constant flux. Risk management must remain top-of-mind for leaders during these uncertain times.
- No one knows what the future of risk management and regulatory compliance has in store for leaders. However, organizations with up-to-date platforms, tools and processes will be the first to detect, mitigate and address risks to the business.
- Our industry experts can help guide your organization as you navigate an increasingly complex risk and compliance landscape and simplify your business processes. Contact us today to get started.



"The next risk frontier is the workforce. I'm talking about behaviors; there are a lot of things that we can control and a lot of things we can automate and safeguard, but we still are a bunch of humans running around executing business to please our clients."

— Kim Curley, Vice President of Workforce Readiness, NTT DATA²²

Sources

1. NTT. "[2021 Global Threat Intelligence Report](#)." 2021.
2. Mathew J. Schwartz. "[Equifax's Data Breach Costs Hit \\$1.4 Billion](#)." Bank Info Security. May 13, 2019.
3. Paul Sandle. "[British Airways faces record \\$230 million fine over data theft](#)." Reuters. July 8, 2019.
4. Mike Isaac, Katie Benner and Sheera Frenkel. "[Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data](#)." New York Time. November 21, 2017.
5. Ponemon Institute. "[The True Cost of Compliance with Data Protection Regulations](#)." Globalscape by HelpSystems. December 2017.
6. NTT DATA. "[How Banks Can Mitigate Risk While Accelerating Digital](#)." March 2022.
7. Investopedia. "[Environmental, Social, and Governance \(ESG\) Criteria](#)." Updated February 23, 2022.
8. Will Kenton. "[Sin Stock](#)." Investopedia. Updated March 4, 2021.
9. NTT DATA. "[NTT DATA Introduces Global Insurance Digital Platform \(GIDP™\) for the Life & Annuity Industry](#)." Press release. November 30, 2021.
10. Jon Hale. "[A Tipping Point for Sustainable Investing](#)." Morningstar. January 23, 2020.
11. MSCI ESG Research. "[Swipe to invest story behind millennials investing](#)." March 2020.
12. MSCI. "[MSCI ESG Fund Metrics Launches on Leading Market Data Platforms](#)." Press release. October 24, 2017.
13. Joe Schifano. "[Building an Effective Surveillance and Compliance Program For the Digital Asset Market](#)." Traders Magazine. March 21, 2022.
14. Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission. "[A Resource Guide to the U.S. Foreign Corrupt Practices Act](#)." Second Edition. U.S. Securities and Exchange Commission. July 2020.
15. U.S. Department of Justice. "[Foreign Corruption Practices Act](#)."
16. Office of the Spokesperson, U.S. Department of State. "[Rewards for Justice – Reward Offer for Information on Foreign Malicious Cyber Activity Against U.S. Critical Infrastructure](#)." Media Note. July 15, 2021.
17. Aaron Holmes. "[533 million Facebook users' phone numbers and personal data have been leaked online](#)." Insider. April 3, 2021.
18. Masha Komnenic. "[Biggest Data Breaches in 2022](#)." Termly. March 25, 2022.
19. SafelyDetectives. "[Amazon Fake Reviews Scam Exposed in Data Breach](#)." May 6, 2021.
20. Lily Hay Newman. "[38M Records Were Exposed Online—including Contact-Tracing Info](#)." Wired. August 23, 2021.
21. Bill Sun. "[No Time Off for Insurance Compliance](#)." NTT DATA Blog. August 24, 2020.
22. NTT DATA Services. "[Bank Modernization in 2022](#)." Video. February 10, 2022.



Visit our website to learn more.

NTT DATA Services is a recognized leader in IT and business services headquartered in Texas. A global division of NTT DATA – a part of NTT Group – we use consulting and deep industry expertise to help clients accelerate and sustain value throughout their digital journeys.