REPRINT

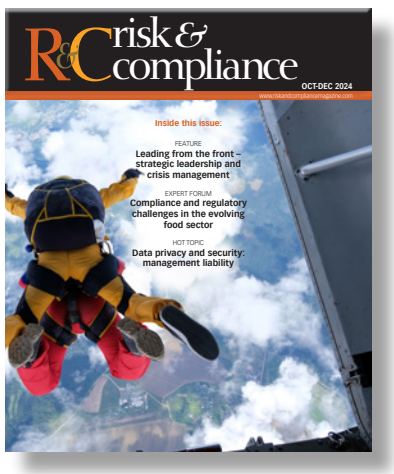
R&C risk & compliance

DATA PRIVACY AND SECURITY: MANAGEMENT LIABILITY

REPRINTED FROM:

RISK & COMPLIANCE MAGAZINE

OCT-DEC 2024 ISSUE



www.riskandcompliancemagazine.com

Visit the website to request a free copy of the full e-magazine

BDO

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

HOT TOPIC

DATA PRIVACY AND SECURITY: MANAGEMENT LIABILITY

PANEL EXPERTS

Matthew White
Shareholder
Baker Donelson
T: +1 (901) 577 8182
E: mwhite@bakerdonelson.com

Matthew White is co-chair of Baker Donelson's financial services cyber security and data privacy team and a member of the incident response team. He regularly advises clients on matters related to cyber security, data privacy, technology and AI. Mr White received his JD from the University of Florida, Levin College of Law.

Taryn Kilkenny Crane
Practice Leader
BDO USA, P.C
T: +1 (301) 354 2583
E: tcrane@bdo.com

Taryn Crane is the privacy and data protection practice leader at BDO USA, P.C. She has a focus in privacy, data protection and privacy technology services, and has consulting experience working across several markets including hospitality, retail, financial services, insurance, technology, life science, industrial and nonprofits. She also has experience advising and delivering privacy programme solutions, ranging from maturity assessments, programme development and technology implementation.

Thomas H. Bentz, Jr.
Partner
Holland & Knight LLP
T: +1 (202) 828 1879
E: thomas.bentz@hklaw.com

Thomas H. Bentz Jr. practices insurance law with a focus on D&O, cyber and other management liability insurance policies. Mr Bentz leads Holland & Knight's D&O and management liability insurance team which provides insight and guidance on ways to improve policy language and helps insureds maximise their possible insurance recovery. He also co-chairs the firm's insurance industry team.

William E. Ridgway
Partner
Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates
T: +1 (312) 407 0449
E: william.ridgway@skadden.com

William E. Ridgway is co-head of Skadden's global cyber security and data privacy practice and a member of the litigation group. He is a former federal prosecutor with extensive trial and investigations experience who advises companies on their most sensitive cyber security, data privacy and white-collar matters.

R&C: How would you characterise current awareness levels among organisations when it comes to safeguarding their data? What are the key risks in this area and how have they evolved in recent years?

White: Given the number of highly publicised cyber incidents, as well as the proliferation of data privacy laws both in the US and abroad, companies are more cognisant than ever of the risks facing their data. We have seen numerous companies focus their time, energy and budgets on hardening their data protection programmes. Especially considering the Securities and Exchange Commission's (SEC's) new cyber reporting rules, for many companies that engagement has gone all the way up to the board level. That said, more can and needs to be done. Data privacy and security threats are constantly evolving and, as a result, companies' programmes need to as well. We continue to face more sophisticated cyber attacks, including increased usage of artificial intelligence (AI), unpredictability in ransomware attacks due to the promulgation of ransomware-as-a-service, an increasing number of attacks on vendors and supply chains, and more and more zero-day attacks. Because of these risks, companies must continue to be vigilant.

Bentz Jr: Most organisations are fairly aware of the risks associated with safeguarding their data. Some companies struggle with costs. For others, the issue is more about balancing the need to gather personally identifiable information for business purposes versus the risks associated with doing so. Many companies have attempted to mitigate their risks by using the cloud or other third-party vendors to keep their data safe. However, the biggest risk is, and has always been, human error. Hackers have become experts on ways to trick people into sharing their passwords or other information in order to gain access to the system. Safeguards such as dual factor authentication and biometric-based passwords have been helpful, but even those solutions are not foolproof.

Ridgway: Increasing regulatory scrutiny and high-profile data breaches have undoubtedly led organisations to become more attuned to the importance of safeguarding data. But a significant gap persists between understanding data security risks and effectively mitigating them. Some of the key risks in this area include the evolving threat landscape, third- and fourth-party vulnerabilities, and human error. Recent years have seen a surge in ransomware attacks, supply chain compromises and data breaches resulting from phishing scams. At the same time, regulators continue to demand prompt escalation, senior-level engagement and notification.

Organisations should adapt their security postures and crisis response procedures to address these dynamic challenges and prioritise proactive risk management.

Crane: Most organisations realise data protection is an area that requires attention. That said, it can be challenging to obtain adequate resources and budget with so many competing priorities. Organisations try to reason or justify their position based on their perceived risk in comparison to other 'obvious targets', like Big Tech. However, with cyber incidents on the rise, and with regulators having left their mark on certain landmark investigations, their lens is widening. Unfortunately, it is common for a company to start investing more heavily in data protection only after it has experienced an expensive data incident or regulatory inquiry. This is often more costly as the risks of non-compliance could include years of remediation, millions of dollars in fines if not more, and reputational damage. Many US laws also allow for class action, which is another source of long-term financial burden.

R&C: Are governments demonstrating a commitment to ensure data protection through legislative measures? Are you seeing a rise in related enforcement?

> **"D&Os need to prioritise understanding data-related liabilities and enhancing their cyber security knowledge."**
>
> *William E. Ridgway, Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates*

Bentz Jr: Legislative measures have been unable to keep up with the rapidly changing reality of how we gather, use and store data. A good example of this is the Video Privacy Protection Act (VPPA). The VPPA was passed in 1988 to protect the rental histories of consumers that rented VHS videos from a brick-and-mortar rental store. Today, plaintiffs' firms argue that any tracking of streaming content on a website is a violation of that law. Obviously, streaming content on a website was not even contemplated in 1988. However, since Congress has been unable to pass new legislation regarding streaming content on consumer websites, plaintiffs

try to cram a square peg into a round hole. Even laws that have passed more recently have struggled to maintain relevance in this rapidly changing environment where advancements in AI and other technologies occur almost daily.

Ridgway: Governments have shown a growing commitment to data protection through a surge of legislative activity in recent years. Regulations such as the European Union's (EU's) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have set global standards for data privacy, which other jurisdictions are emulating. Enforcement actions have also spiked, reflecting the seriousness with which regulators view data protection. Yet challenges such as inconsistencies in global regulations and the need for effective enforcement mechanisms remain. The trend toward stricter data protection regimes is likely to continue, which places increased pressure on organisations to adapt to and comply with an ever-changing regulatory landscape.

Crane: There has been a lot of activity in the last six years since the onset of the EU's GDPR, which set in motion a cascade of global activity to propose and enact similar legislation in many other jurisdictions. The EU continues to set the tone with massive enforcements and continuous lawmaking, with the introduction of more recent regulations like the Digital Services Act and the AI Act. These newer laws raise the bar with larger potential fine amounts per violation. In the US, we do not have a comprehensive federal privacy law, however, each year more states enact their own. At the federal level, the Department of Health and Human Services and the SEC recently amended the Health Insurance Portability and Accountability Act and Regulation S-P, respectively, and the Federal Trade Commission (FTC) has been actively enforcing violations with particular focus on health and sensitive data, consumer transparency, children's privacy and AI.

> **"Since human error is typically the most vulnerable point of a company's data protection strategy, regular training and testing of employees can be a very effective way to limit a company's exposure."**
>
> *Thomas H. Bentz, Jr., Holland & Knight LLP*

White: There have been numerous efforts by domestic and foreign governments to legislate data protection measures. Many of these efforts have been successful internationally, with the passage of laws like the GDPR in the EU and the UK, the Personal Information Protection Law of the People's Republic of China, the Personal Information Protection and Electronic Documents Act in Canada, as well as legislation in Brazil and Australia, among other places. In the US, federal comprehensive data privacy legislation has thus far stalled. Instead, we have seen a proliferation of state privacy laws, including the 2020 California Privacy Rights Act. We are currently up to 19 states that have passed comprehensive privacy legislation. We have also seen industry specific legislation affecting data in healthcare, financial services, education, critical infrastructure and defence, among others. Generally speaking, enforcement actions from regulators are on the rise, as is private privacy-related litigation.

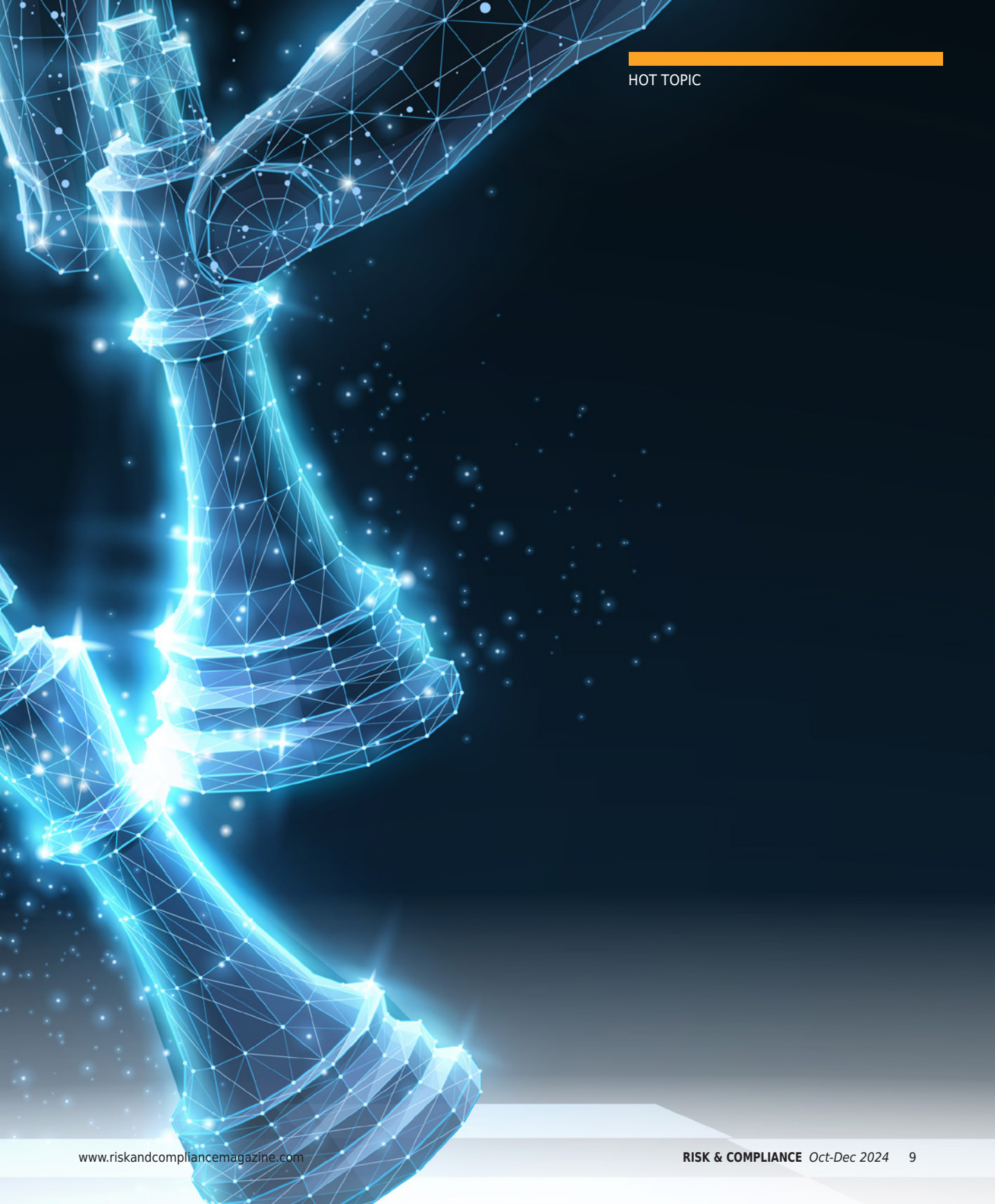
R&C: In the event of a security failure leading to data loss, to what extent do potential liabilities for the board and C-suite come into play?

Ridgway: The potential liability for boards and C-suite executives in the event of a security failure is significant and evolving. While specific liabilities vary by jurisdiction, courts have held that directors' duties of care and loyalty toward a corporation apply to their oversight of cyber security activities. Lawsuits arising from data breaches reflect an emerging expectation that directors must play an active role in cyber security planning and cannot delegate the issue entirely to management. The cases suggest that directors may be held personally liable for failing to ensure proper policies were in place to protect a company or issuing misleading statements about their companies' preparedness. Regulators and investors expect senior management and boards to provide appropriate leadership and oversight of a cyber risk management programme. The increasing complexity of cyber threats and the growing emphasis on data privacy have heightened scrutiny of board and senior management oversight. Organisations should implement robust governance and risk management frameworks.

White: Factors relevant to the analysis of a security failure include the nature of the data, applicable laws and regulations, the adequacy of the company's cyber security measures, the board's and C-suite's involvement in managing those risks, and actions and statements from the company concerning the incident. Boards and C-suites have been found liable under a variety of theories including breach of fiduciary duty negligence, violation of securities laws and violations of data protection regulations. The SEC's new cyber

reporting rules for public companies has highlighted some of these issues, as public companies must now report cyber incidents within four days of determining the incident was material. There have been some prominent examples of the SEC bringing actions against companies and their executives after such reporting and, recently, some initial rulings as to the permissible breadth of those claims. These include charges against Solarwinds and the US District Court for the Southern District of New York's recent dismissal of several of those claims.

Crane: There is case law involving company leaders who have been held personally liable for data breaches. In recent years, the FTC has pursued multiple personal liability charges based on an individual's alleged actions or inactions related to data incidents. In cases like these, the regulators are arguing that the conduct of these individuals is negligent, such as wilful decision making that either avoids or ignores issues and risks which were identified and communicated to those in leadership. It is certainly possible that we will see more of these cases over time. Data incidents are inevitable, so organisations need to demonstrate that they are taking privacy and security seriously and that starts at the top with the board and C-suite executives.



Bentz Jr: Any data incident can lead to liabilities for the board and other C-suite employees. In addition to company losses, third-party lawsuits, and regulatory fines or penalties, directors and officers (D&Os) may also face personal liability for alleged breaches of their fiduciary duties related to their gathering, use and storage of data. This is one reason why it is so important for companies to make sure that their D&O insurance coverage does not exclude claims that are based upon, arising from or in any way related to any type of data incident. This type of exclusion on a D&O insurance policy can subject D&Os to significant personal liabilities.

R&C: What measures should senior management take to bolster their company's data protection strategies? What new privacy features and business processes might this entail?

Crane: A strong data protection strategy starts at the foundation. Senior leaders should first focus on employing qualified and capable data protection leaders who have demonstrated experience building and maintaining a successful data protection programme. The board should be allocating adequate resources and budget to meet obligations, and actively engaged in risk-based decision making to verify that the company's choices are reasonable, responsible and clearly documented. Insist on enhanced data governance and due diligence programmes. Data governance is foundational to both privacy and security because without a strong understanding of your data it is difficult to protect it. Also remember that outsourcing to a third party does not outsource risk. Many data breaches involve third-party providers or company acquisitions. Third party risk management and technical due diligence are critical to evaluating and mitigating risk.

Bentz Jr: Since human error is typically the most vulnerable point of a company's data protection strategy, regular training and testing of employees can be a very effective way to limit a company's exposure. Requiring dual factor authentication for all log-ins and wire transfers is another way to limit exposure. Beyond these things, making sure that the company has strong insurance protection with adequate limits, maintains a well-vetted and reviewed incident response policy, and requires key players to participate in regular tabletop exercises to test their insurance and incident response plans, can also be very helpful. Finally, having agreements in place with both legal and forensic advisers who are approved by the company's insurance programme can limit a company's exposure by ensuring a quicker response in the event of an incident.

White: There are several steps companies can take to bolster their data protection strategies. These

include creating a robust cyber security framework by implementing and maintaining a comprehensive cyber security programme that complies with legal and regulatory requirements. Companies can also conduct a broad data mapping exercise across the organisation to determine what data is collected, where it is stored and how it is shared. Establishing board and C-suite involvement is certainly important, including ensuring active and informed oversight of cyber security risks, including regular updates from the chief information security officer and other relevant teams. Engaging in incident response planning, including developing an incident response plan to address security breaches swiftly and effectively, and then testing that plan through tabletop exercises or simulated cyber attacks is another option. Companies should also consider D&O insurance with specific coverage for cyber security-related liabilities. Finally, it is advisable to ensure that IT and cyber security departments are sufficiently funded to procure necessary technological advancements to better protect the company's data and systems.

Ridgway: Senior management should prioritise data protection by fostering a strong data security culture, investing in robust technology and implementing comprehensive governance frameworks. This generally includes appointing a dedicated data protection officer, conducting regular risk assessments, updating incident response plans and testing those incident response plans through regular tabletop exercises intended to simulate a cyber incident. New privacy features may involve multifactor authentication, data minimisation and anonymisation, and encryption techniques. Additionally, organisations should consider implementing privacy by design principles in product development and adopting transparent data handling practices to build trust with customers.

> **"Not all policies are equal, so organisations should work with insurance advisers to navigate brokers and carriers to understand coverage options and make informed decisions."**
>
> *Taryn Kilkenny Crane, BDO USA, P.C.*

R&C: How important is it for senior management to have recourse to a cyber liability insurance policy with appropriate

coverage? What potential consequences face managers without such a policy?

Bentz Jr: A strong cyber liability insurance policy can be the difference between a company surviving a data incident and insolvency. For some managers, a weak cyber liability policy can cost them their job. We have seen a number of risk managers get fired because the policy they purchased would not allow the insured to hire their preferred law firm or forensic provider. We have also seen this happen when the cyber policy did not provide coverage for social engineering fraud or other cyber risks. This can also be an issue for D&O coverage, when overly broad cyber exclusions on the D&O policy create a gap in the coverage and expose D&Os to potential personal liability in a follow-on derivative or securities litigation. Fortunately, the 'fixes' to these issues are often free upon request or have minimal impact on the premium.

White: Having a cyber liability insurance policy with appropriate coverage is crucial for senior management for several reasons, including that the absence of such a policy can lead to significant consequences. As costs related to a data breach continue to rise exponentially, an appropriate policy can provide financial protection by covering costs associated with a data breach, including notification expenses, legal fees, forensic investigation costs, regulatory fines, business interruption or third-party claims. These policies can also provide access to experts including experienced cyber security lawyers, forensic technology firms, e-discovery companies, negotiators, public relations and more.

> **"Given the number of highly publicised cyber incidents, companies are more cognisant than ever of the risks facing their data."**
>
> *Mattew White, Baker Donelson*

Ridgway: Cyber liability insurance can serve an important role for a company. It provides a financial safety net against the potentially catastrophic costs of a data breach. Without adequate coverage, potential consequences could include substantial financial losses, legal liabilities and reputational harm. Insurance offers crucial support for incident response, legal defence and business recovery

efforts. While it is not a substitute for robust security measures, it is vital to a comprehensive risk management strategy.

Crane: Cyber insurance is not a replacement for a strong data protection programme, but it is critical for offsetting financial losses. Without it, companies could be exposed to significant financial burden resulting from the costs of investigation, analysis, notification, credit monitoring, litigation and other remediation activities. While premiums have risen and issuers are more selective about who they will insure, the market has stabilised and premiums are rising at steadier growth rates. By demonstrating the strength of a company's data protection programme, insurers may be able to reduce premiums. That said, not all policies are equal, so organisations should work with insurance advisers to navigate brokers and carriers to understand coverage options and make informed decisions. For example, some policies may not include ransomware attacks or business interruption, so organisations should understand their coverage and weave this into their risk mitigation strategy and annual tabletop exercises.

R&C: What essential advice would you offer to D&Os on understanding data-related liabilities and increasing their cyber security knowledge?

Crane: D&Os should make data protection a board-level topic and appoint someone to the board who has a data protection background. They should also establish specific committees or oversight boards to steer the direction of data protection activities at the organisation. Have the information security officer and privacy officer report on the programme performance and educate the board on the risks currently impacting the organisation. Companies should also seek external opinions or third-party assessments to review programme maturity annually and demonstrate progress year over year. It is not a matter of if but when a data incident will impact an organisation. Therefore, companies should be proactive to implement privacy and data protection controls that will hopefully minimise the impact when one occurs. Keep in mind that personal liability is most often due to negligence, so it is important for companies to be able to demonstrate good intention, ongoing due diligence and reasonable decision making when regulators conduct their investigation.

Ridgway: D&Os need to prioritise understanding data-related liabilities and enhancing their cyber security knowledge. They should begin by understanding governance around relevant data protection laws and regulations, such as the GDPR and CCPA. They should also consider attending cyber security training and workshops to better

understand the evolving threat landscape, and engaging with their organisation's IT and security teams to gain insights into the organisation's cyber security posture. D&Os should understand their organisation's data assets, the value of those assets and the potential consequences of a data breach. By proactively addressing these areas, D&Os can better mitigate risks and satisfy their fiduciary duties.

White: D&Os must be engaged and actively manage data-related liabilities by understanding cyber security risks, legal obligations, third-party risks and their fiduciary duties. They should enhance their cyber security knowledge through continuous education and engagement with experts, as well as hiring experienced personnel. Implementing strong governance practices, ensuring adequate resource allocation, appropriately testing and auditing, and promoting a cyber security culture are crucial. Regularly reviewing cyber insurance and incident response plans, conducting testing and auditing, and participating in crisis simulations are essential. D&Os should lead by example by increasing their cyber security knowledge, implementing strong governance practices and ensuring that the company is well-prepared for cyber threats – thus effectively protecting the company and themselves from potential liabilities and reputational damage associated with a cyber attack.

Bentz Jr: The law does not require that each D&O at a company become a cyber security expert. To obtain the protections of the business judgment rule, D&Os must act on an informed basis, in good faith and in the honest belief that the action was in the best interest of the company. Acting on an informed basis is key to this equation. D&Os should be sure that they are getting regular reports on their cyber security risks and exposures, that they have and regularly evaluate the company's plans to act promptly and appropriately in the event of a cyber incident, and that they document their decisions regarding cyber matters and the reasons behind those decisions.

R&C: Looking ahead, what predictions would you make for the data privacy and cyber security landscape? What repercussions are these trends likely to have for management liability?

Ridgway: The data privacy and cyber security landscape is evolving rapidly. We expect increased regulatory scrutiny, sophisticated cyber attacks and a heightened focus on data protection by design. With the rise of AI and proliferation of connected devices, new challenges and vulnerabilities are sure to arise. These trends will alter management liability. D&Os can expect increased personal exposure to legal actions, reputational harm and financial losses

in the event of a data breach or tech-related crisis. Proactive risk management, including robust cyber security measures and comprehensive insurance coverage, will be vital to mitigating these risks.

White: Over the next few years, the data privacy and cyber security landscape will continue to see rising cyber threats, increased regulatory scrutiny and greater consumer protections regarding data control. On the cyber security front, we will continue to see an increased number of cyber attacks. These attacks will be increasingly driven by advanced technologies like AI. At the same time, companies are collecting and maintaining more data than ever, which leaves them more vulnerable to significant financial and operational impacts, increasing the pressure on management to implement robust cyber security measures. On the regulatory side, governments and regulatory bodies worldwide are tightening data protection laws and increasing enforcement, particularly with respect to the rise of AI, the internet of things, children's data, online tracking and marketing tools, and big data analytics. The sheer volume of these laws and regulations creates a complicated framework in which companies need to ensure they are remaining compliant. Similarly, evolving privacy rights will further complicate compliance. Consumers and employees will continue to demand greater control over their personal data, leading to more comprehensive data protection laws and additional privacy rights for individuals. Management will need to navigate this complex privacy landscape, with increased liability risk if they fail to protect personal data adequately or violate privacy rights. These trends will heighten liability risks, necessitating proactive engagement and robust governance to protect companies and their leadership.

Bentz Jr: It is likely that the federal government will continue to struggle to pass meaningful, cyber security related legislation – at least in the near future. However, in the absence of Congressional action, federal regulators such as the FTC and SEC will continue to pass and enforce regulations to address cyber security issues. We also expect that states will continue to push various laws to address their main concerns on a state-wide level. Cookies, pixels and child privacy issues, including how children access and interact with online platforms, will continue to dominate the focus of both legislators and litigators in the short term, whereas we expect that issues related to the use of AI will begin to create additional long-term exposures for D&Os.

Crane: Cyber incidents are going to continue to multiply, especially as bad actors evolve their attack strategies to include new methodologies and enhanced technology like generative AI. Regulators

are likely to continue proposing and passing laws which aim to address these issues and hold organisations accountable for protecting personal data. However, they are unlikely to keep pace with the technology advancements, and organisations will continue to juggle compliance across the patchwork of global and domestic privacy laws. When incidents do occur, the actions or inactions of the board, officers and other senior leaders will likely be under scrutiny to determine whether there were failures to implement proper controls, monitoring or reporting of data protection issues or risks. Management should be proactive and prioritise a robust data protection programme before it becomes a problem, not after. R&C