FORTRA™

6 Cybersecurity Thought Leaders on Data Protection

Expert Views on the Challenges of Today & Tomorrow

Table of contents

INTRODUCTION 3

CURRENT DATA PROTECTION CHALLENGES 4

- Sarah Norford-Jones 6
- Gary Hibberd 8
- Piers Chivers 10
- Ambler T. Jackson 12
- Camilla Winlo 14
- Jarell Oshodi 16

CRITICAL CHALLENGES IN THE COMING YEARS 17

- Sarah Norford-Jones 18
- Gary Hibberd 19
- Piers Chivers 20
- Ambler T. Jackson 21
- Camilla Winlo 21
- Jarell Oshodi 22

OVERCOMING DATA PROTECTION CHALLENGES 23

- Sarah Norford-Jones 24
- Gary Hibberd 24
- Piers Chivers 25
- Ambler T. Jackson 26
- Camilla Winlo 26
- Jarell Oshodi 27

HOW TO ENGAGE BUSINESS LEADERSHIP FOR DATA PROTECTION SUPPORT 28

- Sarah Norford-Jones 29
- Gary Hibberd 29
- Piers Chivers 30
- Ambler T. Jackson 31
- Camilla Winlo 31
- Jarell Oshodi 32

CREATE CORPORATE-WIDE AWARENESS 33

- Sarah Norford-Jones 34
- Gary Hibberd 34
- Jarell Oshodi 35

HOW BUSINESS LEADERS CAN PARTICIPATE TO CREATE SUCCESS 36

- Sarah Norford-Jones 37
- Gary Hibberd 37
- Ambler T. Jackson 38
- Camilla Winlo 38
- Jarell Oshodi 38

CONCLUSION 39

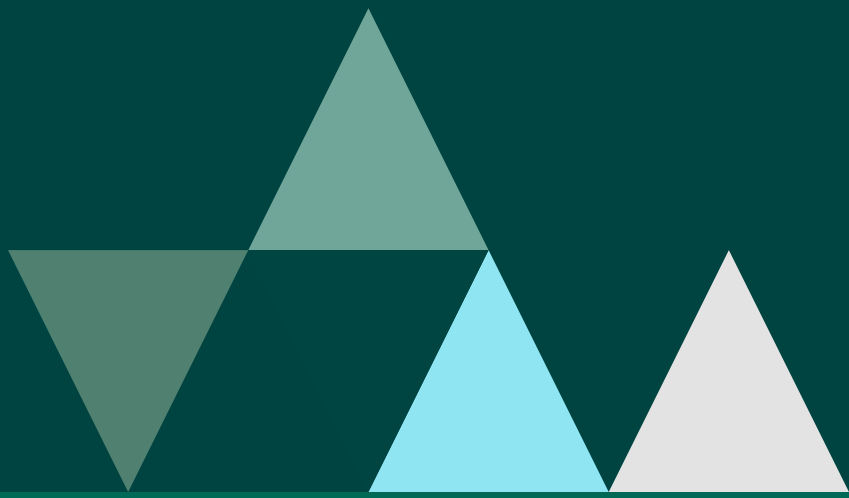
Introduction

If you were asked to tally up the value of every asset in your organization, while it might be a daunting task, it would be relatively achievable. Every asset has a tangible value, whether it's the office furniture or equipment, right down to the fixtures. Even employee salaries can be calculated against sunk costs, depreciation, and amortized value. However, the value of the data on which the organization runs is not as easily quantified.

Data can have different values for different purposes. A client mailing list has value that differs from an accounting database. What price can be placed on the value of protecting the privacy and confidentiality of the data? Many regulations have sought to impose fines for data protection violations, but not until various due process is followed.

Similarly, it is impossible to calculate the harm that can come to breach victims, whose information can be sold to multiple parties for varying criminal endeavors.

Data protection is important for the survival of any organization. Getting the support of corporate leadership is essential to protecting an organization's sensitive data. We spoke with six experts about their impressions of the current challenges surrounding data protection and what the future may look like, as well as ways to gain support within an organization for a data protection initiative.



Current data protection challenges

Data protection starts by examining what it is that you want to protect, and why. Are your challenges centered around regulatory compliance, technological hurdles, the changing attack methods of cybercriminals, or perhaps a combination of all of those? We started by seeking the answer to the following question:

In your industry, what are the most significant challenges you face regarding data protection?

Current data protection challenges

Sarah Norford-Jones

Co-Founder and Chief Marketing Officer, YEO Messaging

Current data protection challenges

Sarah Norford-Jones

Co-Founder and Chief Marketing Officer, YEO Messaging

Data protection is one of the most pressing challenges facing most industries today. In an increasingly digitized world, where data sharing has become an integral part of everyday life, the onus is on providers to ensure that customers' data is protected. Data protection laws are now in place to ensure that companies protect user data and information, both from malicious actors and from their own internal processes. The challenge comes in how to best protect user data. Companies must balance user security with the need for convenience and ease of use.

Current data protection challenges

Gary Hibberd

Professor of Communicating Cyber

Current data protection challenges

Gary Hibberd

Professor of Communicating Cyber

One of the most challenging aspects of data protection is the rapidly evolving nature of cyber threats. To put it simply, attackers are finding new ways to exploit the human and technical vulnerabilities in our ever-expanding digital universe. The attack surface is increasing both in terms of people and the devices we use on a day-to-day basis. As people, everyone is fighting for our attention, including our employers, customers, and clients – and with this volume of increasing digital distraction, the cyber criminals and threat actors are using this to cover their tracks or modes of attack.

Current data protection challenges

Piers Chivers

Product Manager, Fortra

Current data protection challenges

Piers Chivers
Product Manager, Fortra

I see this as two challenges. The first is that the requirements are often vague. Customers don't necessarily know what they want to protect, which is ironic when you think about it, and the people running the data protection projects have not had good direction from their leadership on what the threats are that need to be addressed.

Secondly, many customers have challenges with the configuration, operation, and use of data protection tools. There are two distinct sets of users here: operators and end users. The operators have a myriad of different tools to manage, and they tend to be complicated tools that need a specialist's knowledge to set up and configure.

Likewise, end users find data protection tools difficult to use. Data protection is not their thing, that's not what they care about. It is not their primary job, so we have to, as much as possible, make the data protection tools work for the benefit of the users while achieving the aim of the business.

Current data protection challenges

Ambler T. Jackson

Cybersecurity Engineer, Noblis

Current data protection challenges

Ambler T. Jackson

Cybersecurity Engineer, Noblis

One of the most significant data protection challenges facing private and public organizations is implementing a data governance strategy that helps stakeholders fully understand the organization's data, e.g., the type of data, how it is used, where it is located within the enterprise, and how it is accessed.

Current data protection challenges

Camilla Winlo

Head of Data Privacy, Gemserv

Current data protection challenges

Camilla Winlo

Head of Data Privacy, Gemserv

The most significant challenge facing data protection is the pace of change to laws and guidance, technology, and the threat landscape.

New and updated data protection laws seem to be announced all the time. Each organization affected by these laws needs to understand the practical impact of the changes on their company. The laws generally share the same underlying principles, but where requirements are different, each organization needs to decide whether to adopt a shared standard across their global business or whether to allow different countries to handle things differently. It's a lot to keep on top of.

Technology is also constantly moving forward, and there can be sudden changes where a technology very quickly becomes popular. We saw that at the start of the pandemic with the technologies to support remote working, and we are seeing it again now with generative learning AI. Organizations need to assess the impact on their business, including how their employees, suppliers, and clients will use the technology, and the risks associated with it.

Cyber criminals are just as innovative as technology firms, and new threats are emerging all the time. But threats don't need to be malicious – new threats emerge when new technologies come out, because of the ways people choose to use them and the mistakes they may make.

It's really important that organizations give data protection teams the resources to stay on top of these changes.

Current data protection challenges

Jarell Oshodi

Deputy Chief Privacy Officer, Centers for Disease Control and Prevention

Current data protection challenges

Jarell Oshodi

Deputy Chief Privacy Officer, Centers for Disease Control and Prevention

Some of the most significant challenges regarding data protection include the always changing and always challenging regulatory landscape, emerging technologies, and employee training and awareness. As privacy professionals, we must stay abreast of and ensure compliance with rapidly changing laws and regulations. These regulations also require continuous monitoring, interpretation, and adaptation of privacy practices. The emergence of new technologies like artificial intelligence and machine learning have introduced unique privacy challenges. Privacy professionals must conduct comprehensive privacy impact assessments to recognize the privacy implications of these technologies and ensure that privacy is built into the design and deployment processes.

Critical challenges in the coming years

Like all security strategies, nothing remains static. Not only are data storage strategies changing, but even the methods for creating data are evolving. Likewise, the various ways of protecting data has to be future-proofed to address these transitional moments. Our experts were asked to peer ahead to answer the question:

What are the most critical challenges for data protection in the coming years?

Critical challenges in the coming years

Sarah Norford-Jones
Co-Founder and Chief Marketing Officer, YEO Messaging

One of the key challenges facing data protection in the coming years will be how to protect data from malicious actors while enabling users to securely access it from multiple devices. As more and more of our lives becomes digitized, it's essential that data is protected both in terms of encryption and identity verification. Scammers and fraudsters are only getting more sophisticated in their methods, and companies and individuals must stay one step ahead.

Another critical challenge will be to integrate more procedures, such as biometric authentication, into the user experience. This will enable companies to ensure that only authorized individuals can access data, while also allowing users to maintain seamless control over their own data.

Critical challenges in the coming years

Gary Hibberd
Professor of Communicating Cyber

The challenges will always remain the same; perception of cybersecurity as an IT problem, and not a business risk. But as Artificial Intelligence (AI) improves, and our reliance on another form of technology increases, the old adage of "in screens we trust" must be tested. We need to remind ourselves that as we harness technology for our own ends, so do cyber criminals and threat actors. We have already seen how dangerous disinformation can be, with how AI generated photos of an attack on the Pentagon caused a dip on the stock markets. This technology is freely available and will most likely be used for political or financial gain in the future.

Critical challenges in the coming years

Piers Chivers
Product Manager, Fortra

Simplification of operation is key. We need to lose all those technical terms and start talking in use cases. That's the way that the end user or the customer generally thinks. Wouldn't it be great if the data protection tools started accepting spoken input? For example, the operator might say “configure my data loss prevention product so that only confidential and personally identifiable information is allowed out of the business if it's sent by Alice Smith”. Wouldn’t it be great if the business could just say that spoken input and get that result?

Another challenge is really a topical subject; Artificial Intelligence (AI) and machine learning will have a huge impact on data protection. Data protection technology is mostly about observing abnormal patterns. For example, an employee who rarely sends zip files out of the business on a Friday, and then all of a sudden is seen transferring zip files, will be seen as an unusual event. Machine learning and AI are especially good at working with patterns and recognizing those abnormal patterns. Of course, the flip side is that the criminals will also be using their own AI and machine learning, so we need to expect that our machine learning must learn before their machine learning. The AI technology used by the bad actors will be trying different types of attacks, and continually probing to try and get around our defenses. It is a real challenge for everyone involved in data protection.

Critical challenges in the coming years

Ambler T. Jackson

Cybersecurity Engineer, Noblis

In the coming years, the most critical challenge for organizations will be maintaining a comprehensive data inventory; such that organizations have a clear path forward for how to protect the voluminous amounts of data that will be collected and processed, and keep pace with all of the data privacy laws and the regulatory compliance landscape.

Camilla Winlo

Head of Data Privacy, Gemserv

The most critical challenge for data protection is ensuring it continues to be seen as relevant and valuable. When potentially transformative new technologies like generative AI are launched, it can be easy for organizational leaders to get excited by the opportunities and struggle to engage with the data protection risks. The conversations around new technologies can be quite esoteric, and when the conversation is about the risk of AI robots destroying humanity, or the lawful basis for collecting the underlying data set, it can be hard for people to relate that to their business and everyday lives. There needs to be more conversation about what the potential impact of personal decisions can be and what kinds of risks people can face through their personal data protection choices.

Jarell Oshodi
Deputy Chief Privacy Officer, Centers for Disease Control and Prevention

> **Public trust and transparency, in general, are crucial challenges we must prioritize. Maintaining public trust and confidence in data protection practices is more important than ever.**

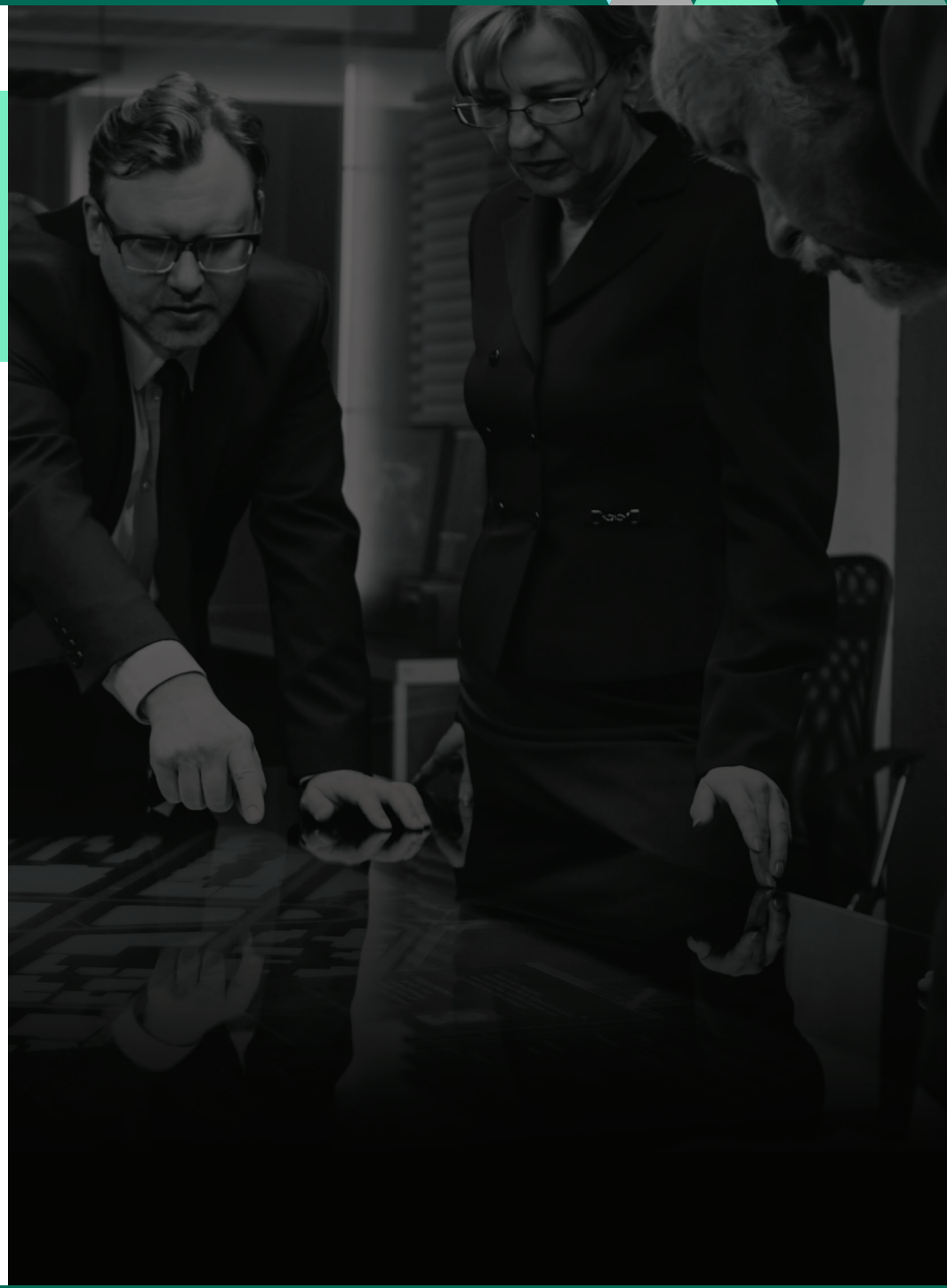
The increasing use of AI and algorithms in decision-making processes will continue to raise concerns regarding privacy, fairness, and transparency. Privacy professionals will need to ensure that data used in AI models are ethically sourced, that individuals' privacy rights are respected, and that algorithmic decision-making processes are fair, explainable, and accountable.

With the growing emphasis on data subject's rights to control their personal data, organizations are focusing on different ways to manage and respect these rights, including those of employees. Privacy professionals are establishing transparent processes for obtaining and managing consent, enabling individuals to exercise their rights easily, and ensuring organizations have mechanisms in place to respond to data subject's requests efficiently, including trust centers.

Overcoming data protection challenges

Often, when asked to predict the future, even the best experts can launch into flights of fancy. To get more insight, we asked:

When reflecting on the most critical challenges for data protection in the coming years, how might these be overcome or prevented?



Overcoming data protection challenges

Sarah Norford-Jones

Co-Founder and Chief Marketing Officer, YEO Messaging

Companies must remain vigilant and use a combination of strategies. It's important to ensure that the highest levels of encryption are used and regularly updated, while also incorporating additional security layers such as biometric authentication. According to the 2023 Data Breach Investigations Report by Verizon, human error is the main cause of 74% of cyber security breaches. Which means, if human error was eliminated entirely, 19 out of 20 cyber breaches may not have ever taken place.

Gary Hibberd

Professor of Communicating Cyber

The language we use with the cybersecurity sector must change, so that we are talking about safety rather than just security. Road safety, and health and safety are concepts people understand, but security has for too long sat within the realm of IT, and therefore it is perceived as boring and technical. Of course, there is a technical aspect to being safe online, but we need to make it as easy as possible to implement security, so that people don't need to think of it.

Piers Chivers
Product Manager, Fortra

The use of voice input to configure data protection tools will make an enormous difference. People tend to articulate effectively about what they want. It is much more difficult for a person to write a configuration rule. The tools generally have a prescriptive way to achieve the end result. However, often the prescriptive way is not quite what the user wants. Changing this could be a huge step going forward by allowing the person to literally say what they want from a data protection perspective.

Another way to address the challenges is to have a set of data protection tools that can collaborate as a whole. For example, wouldn't it be great if a data at rest discovery tool, upon finding a particular file share that has confidential intellectual property, could then initiate a vulnerability assessment data protection tool? The vulnerability assessment tool could then check the permissions on that file share, and make sure they are set for the correct access.

Overcoming data protection challenges

Ambler T. Jackson

Cybersecurity Engineer, Noblis

> **Developing a data protection strategy that includes secure technology which will automate the process of discovering data and enable categorization and mapping will help organizations overcome data protection challenges.**

Camilla Winlo

Head of Data Privacy, Gemserv

Data protection specialists need to make sure we keep up with technologies and threats, and can explain data protection risks in a way that is easy to understand and makes sense to the person in front of you. We also need to be able to explain how to make risk-based decisions and address risks in a way that is equally easy to understand and follow.

Overcoming data protection challenges

Jarell Oshodi

Deputy Chief Privacy Officer, Centers for Disease Control and Prevention

To address privacy challenges, privacy professionals can implement strategies like ensuring that data used for AI models is obtained in a transparent and ethical manner, with proper consent and privacy protections. Regular audits and assessments of AI systems should be conducted to identify and mitigate potential biases or discriminatory outcomes. Comprehensive data subject request management systems should be developed that allow for efficient and timely responses.

Other strategies include implementing privacy-by-design principles to embed data subject rights and privacy protections into organizational practices and systems. Provide clear and user-friendly privacy notices and information to individuals, explaining how their personal data is used and protected. Foster a culture of accountability and ethical data handling within organizations, ensuring privacy practices are upheld at all levels. Invest in continuous education and training for privacy professionals to stay up-to-date with evolving technologies, regulations, and best practices.

How to engage business leadership for data protection support

Business leaders are tasked with high-level concerns that surround a business. These can include everything from real estate negotiations, financial obligations, legal responsibilities, and the future of the organization. It is not often that a technology professional gets more than a few minutes to express the importance and necessity of a new program. Our panel shared their advice about:

how people can gain leadership engagement and support for data protection tools and programs.

How to engage business leadership for data protection support

Sarah Norford-Jones

Co-Founder and Chief Marketing Officer, YEO Messaging

The best way to gain leadership engagement is to explain the importance of data protection, and provide a clear business case as to why it is necessary. For example, data protection can help protect the company from legal and financial liability in the case of a data breach. Additionally, it can help to protect the reputation of the business, as customers' trust in the company is essential for long-term success.

Gary Hibberd

Professor of Communicating Cyber

One of the core skills that consultants like us have is that we know what it means to run a business. We look at the people around the boardroom table and ask "Why would they care about [insert topic]?" The answer to that question is different for each person in the room. They each have a personal agenda, so learn what their "hot spots" are, and hit them. Explain in clear business terms why it's important, but don't overdo the "share and scare" tactic. Yes, there are some scary stats out there, but focus on the positives. No one goes to the gym because we're told "Hey, you'll be unfit and die young!" We're told that we'll feel great, that our clothes will fit better, and we may meet the person of our dreams! They sell a future state that we want to be part of. Use the same tactic to sell your program, or the benefits of your tool. Even if the message is *"You'll sleep better at night and you'll have a full weekend with your family, because we won't need to disturb you!"*

How to engage business leadership for data protection support

Piers Chivers
Product Manager, Fortra

Engaging business leadership takes two distinct approaches. Firstly, there's trust, and then secondly, there is value. When you suggest that you can provide data protection, leaders want to know that you've done it before, that you have the experience, that you have experienced professional services folks that have worked in the industry, and you can provide case studies to provide evidence of your success. That's important for trust. Value is where you can evidence that the money that the leaders are about to spend on your tools will show a tangible return on investment for them. It's key for the leaders to know that they are spending their money effectively, and every data protection tool should have the ability to show the value that is being provided. It would be great if the leadership team can say "how many times has my confidential intellectual property left the business inappropriately," and get a result: A chart, a spreadsheet, a PDF, maybe even a spoken reply to give them the answer. Trust and value are key to gaining leadership engagement.

How to engage business leadership for data protection support

Ambler T. Jackson

Cybersecurity Engineer, Noblis

While leadership is becoming more aware of how the lack of a strong data protection program might impact their organization, in many cases, data privacy, information security and business stakeholders will need to thoughtfully connect the dots between their respective roles and responsibilities and their leadership's desired outcomes for the organization in order to gain their support for data protection tools and programs.

Camilla Winlo

Head of Data Privacy, Gemserv

The most important thing is an ability to relate to the organization's pressures and goals. We also often need to get better at measuring our impact. That's both in terms of reassuring boards that we understand the commercial outcomes of data protection decisions, and in terms of measuring our contribution to ethical objectives.

How to engage business leadership for data protection support

Jarell Oshodi
Deputy Chief Privacy Officer, Centers for Disease Control and Prevention

> **Gaining leadership engagement and support for data protection tools and programs requires highlighting the benefits, risks, and value of investing.**

Engage Leaders in Risk Management Discussions: Involve leaders in discussions on risk management and emphasize how data protection is a crucial aspect of risk mitigation. Present risk assessments and threat scenarios to illustrate the potential impact of data breaches.

Educate Leaders on the Importance of Data Protection. Provide leaders with clear and compelling information about the importance of data protection in our current and future data landscape.

Show Return on Investment (ROI): Develop metrics and key performance indicators (KPIs) that demonstrate the ROI of data protection investments. Measure and report on the effectiveness of data protection tools and programs, such as reduction in data breaches, improved incident response times, increased customer trust, and regulatory compliance.

Create corporate-wide awareness

The C-Suite is always accountable for the activities that happen under their direction. However, data protection is a shared responsibility, and some of our panel of experts expressed ideas about how to engage the entire organization to make data protection part of the corporate culture.

Create corporate-wide awareness

Sarah Norford-Jones

Co-Founder and Chief Marketing Officer, YEO Messaging

It is of utmost importance to continue to educate not only the users of our platforms, but every employee within the company, on the importance of cybersecurity and data protection. Everyone must be aware of the best practices, and understand how their data is being used and protected. Put in place tests, reviews, or check-ins; whatever it takes to educate and ensure everyone within the business understands the importance of data protection.

Gary Hibberd

Professor of Communicating Cyber

All cybersecurity courses should include a section on ethics, privacy, and data protection. In a perfect world, every academic discipline would include the same. From law school, to MBAs, there should be a cybersecurity (cyber safety) module so that we take cyber away from the tech lab, and into the boardroom to stay consistent.

> **We need to stop seeing this as a people problem or seeing better technical devices as the only solution. Our mindset needs to change, both within cybersecurity sector and in the boardroom.**

Create corporate-wide awareness

Jarell Oshodi
Deputy Chief Privacy Officer, Centers for Disease Control and Prevention

Statistics show employees are the leading cause of personally identifiable information (PII) leakage incidents. Privacy professionals need to educate and train employees on privacy best practices, policies, and procedures in an engaging manner in order to build privacy champions. Ensuring that employees understand their roles and responsibilities regarding data protection, promoting a privacy-conscious culture, and regularly updating training programs are essential to mitigate internal privacy risks.

Privacy professionals will need to prioritize transparency, clearly communicate privacy practices to individuals, and provide accessible information about how personal data is collected, used, and protected. Building and maintaining trust through accountable and ethical data handling will be paramount.

How business leaders can participate to create success

Once a data protection strategy is put into place, it should not become the sole responsibility of the technology teams. Business leaders need to be active champions of whatever data protection approach is chosen. By taking a functional interest in the program, the organizational leadership can substantiate the importance of the program. We asked our experts what they would want to see from business leader to validate the data protection process.

How business leaders can participate to create success

Sarah Norford-Jones

Co-Founder and Chief Marketing Officer, YEO Messaging

Leadership must be willing to invest the necessary resources into data protection initiatives and ensure they are taken seriously within the organization. It's important to ensure that data protection is not seen as a "tick-box" exercise, but rather an ongoing process that requires regular review and updating. Leadership must ensure that it's incorporated into the company culture, and that everyone within the business is aware of their responsibilities when it comes to data protection. By doing this, leadership will be sending a clear message that data protection is not only critical, but also a priority. This will help to ensure that the company is well-positioned to protect user data. Data protection is a critical part of any company's security strategy, and it needs to be championed from the top down.

Gary Hibberd

Professor of Communicating Cyber

At the moment, the role of CISO is leading to Business Information Security Officer (BISO), but the role of a Chief Data Officer (CDO) will undoubtedly become increasingly important, as this role focuses on how an organization uses data, and includes ethical considerations as well as technical requirements to protect it.

How business leaders can participate to create success

Ambler T. Jackson

Cybersecurity Engineer, Noblis

The process of creating and maintaining a data inventory is not one that the organization can engage in once, never to revisit again until there is an audit, or worse, a data breach. The process is continuous.

Camilla Winlo

Head of Data Privacy, Gemserv

When we make a recommendation or raise a concern, it is much more likely to be heard and taken seriously if we have a demonstrable track record of being able to explain the issue in a way that helps leaders make the right decision, and being able to demonstrate the impact of following our advice.

Jarell Oshodi

Deputy Chief Privacy Officer, Centers for Disease Control and Prevention

Engage leaders in identifying and prioritizing data protection risks specific to the organization's industry and operations. Include tabletop exercises to help them understand the roles of stakeholders. Explain the potential risks and consequences of data breaches, regulatory non-compliance, and damage to reputation. Help leaders understand how data protection aligns with organizational goals, values, and strategic objectives.

Conclusion

What is your data worth? Unlike the physical assets of an organization, the value of data is not easily quantifiable. Regulations have set bold attempts in motion to keep up with data protection, but the technology is progressing faster than any regulatory body or standards organization can rival.

The experts we selected have broad experience in the data protection field. They work with the technologies that can protect an organization, and they also interact with the people at all levels of the organization who are the stewards of that data. The insights and knowledge that they shared is invaluable towards helping in your data protection practice.

Fortra's Data Protection

Interlocking solutions that protect sensitive data while keeping users productive. Our Data Protection tools can be SaaS deployed or on-premises, and we offer managed services to extend your team and reduce risk.

Learn more on our website.

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

 | fta-dg-ebook-0823-r1-an