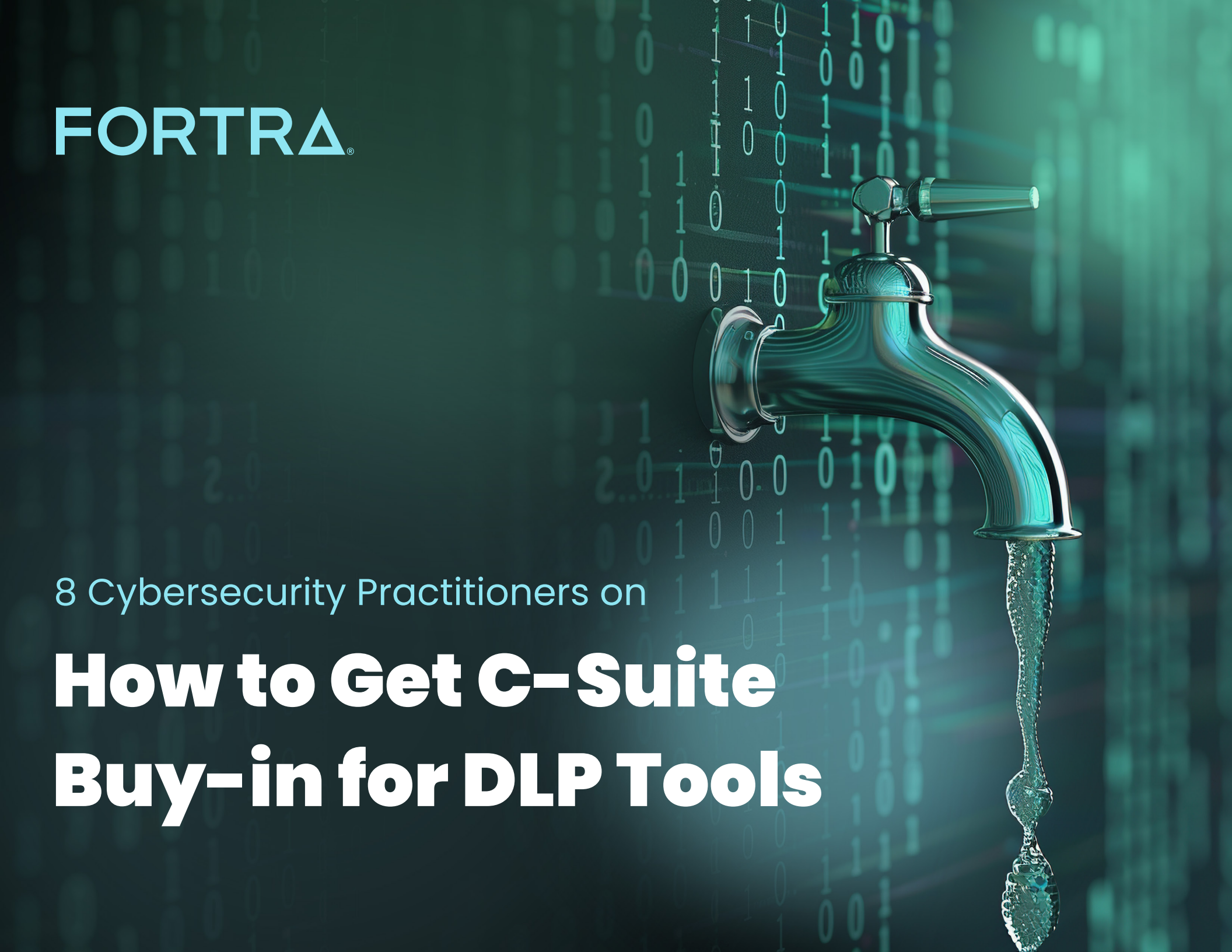
FORTRA



8 Cybersecurity Practitioners on

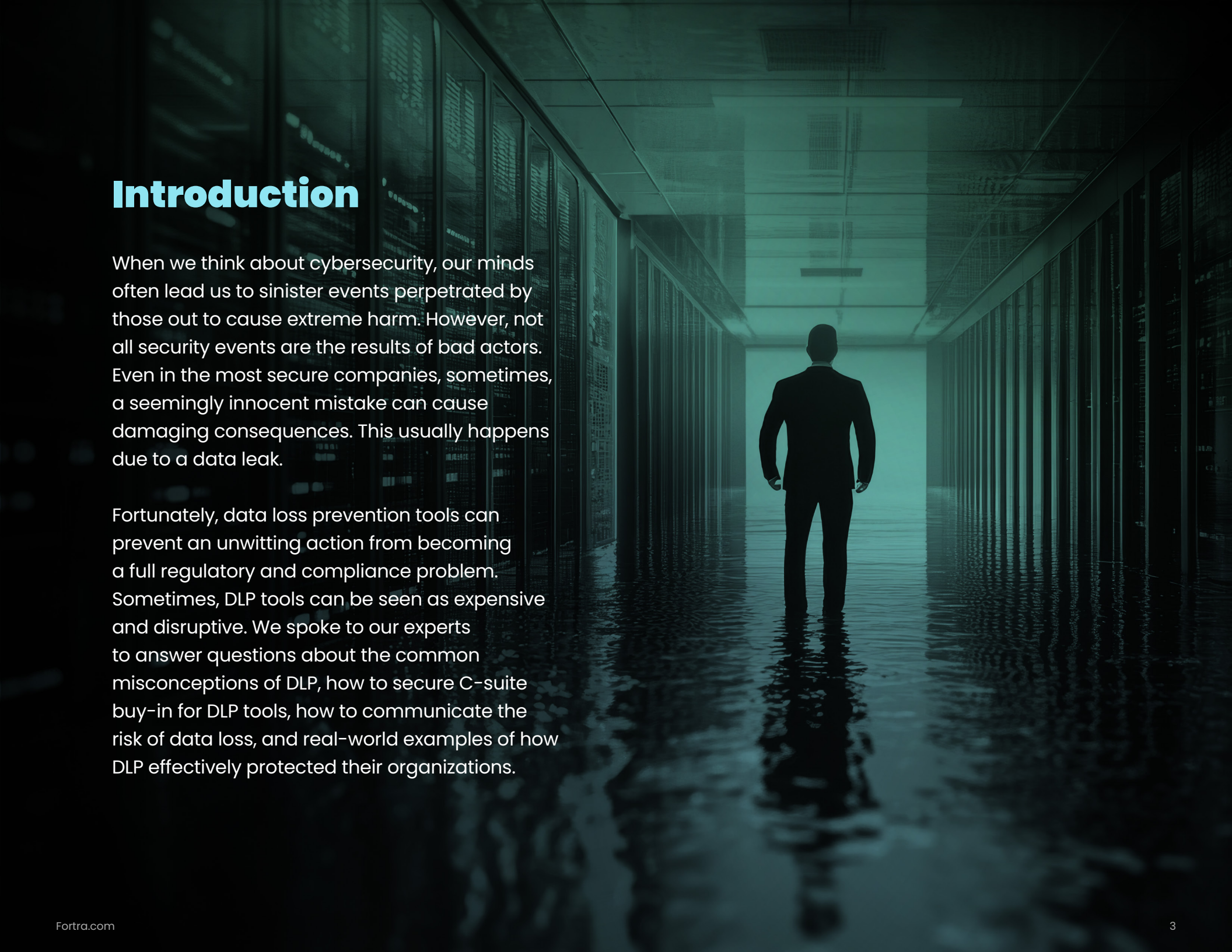
How to Get C-Suite Buy-in for DLP Tools

Table of contents

Introduction

When we think about cybersecurity, our minds often lead us to sinister events perpetrated by those out to cause extreme harm. However, not all security events are the results of bad actors. Even in the most secure companies, sometimes, a seemingly innocent mistake can cause damaging consequences. This usually happens due to a data leak.

Fortunately, data loss prevention tools can prevent an unwitting action from becoming a full regulatory and compliance problem. Sometimes, DLP tools can be seen as expensive and disruptive. We spoke to our experts to answer questions about the common misconceptions of DLP, how to secure C-suite buy-in for DLP tools, how to communicate the risk of data loss, and real-world examples of how DLP effectively protected their organizations.



The Minds Behind the Insights

Our eBook is made possible by a group of accomplished cybersecurity professionals who bring years of experience, insights, and practical wisdom. These experts come from diverse backgrounds across the cybersecurity landscape, each contributing a unique perspective on data loss prevention, compliance, and security best practices.

Their knowledge is invaluable in shedding light on how real-world organizations use DLP to protect sensitive data, mitigate risks, and navigate today's complex threat environment. We're excited to share their expertise with you!

The Minds Behind the Insights

Ross Moore

Cyber Security Support Analyst with Passageways

Ross Moore

Cyber Security Support Analyst with Passageways

Ross Moore is the Cyber Security Support Analyst with Passageways. He has experience with ISO 27001, ISO 27701, and SOC 2 Type 2 implementation and maintenance.
Over the course of his 20+ years of IT and Security, Ross has served in a variety of operations and infosec roles for companies in the manufacturing, healthcare, real estate, business insurance, and technology sectors.
He holds ISC2's SSCP along with CompTIA's Pentest+ and Security+ certifications, a B.S. in Cyber Security and Information Assurance from WGU, and a B.A. in Bible/Counseling from Johnson University.

The Minds Behind the Insights

Dr. Alea Fairchild

Research Fellow at
The Constantia Institute

Dr. Alea Fairchild

Research Fellow at
The Constantia Institute

Dr. Alea Fairchild is a seasoned expert in workplace technologies and cybersecurity, dedicated to enhancing organizational efficiency while safeguarding critical data. With over a decade of experience, Alea specializes in advising on innovative tech solutions that streamline business processes. Her passion for empowering teams through technology has made her a sought-after speaker and consultant in the industry.

Her thought leadership extends to emerging trends in sensory technology and its applications in enhancing workplace environments, demonstrating her commitment to fostering innovation that prioritizes both productivity and safety.

The Minds Behind the Insights

Wade Barisoff

Director, Product Management, Data Protection, at Fortra

Wade Barisoff

Director, Product Management, Data Protection, at Fortra

Wade Barisoff is a Director of Product at Fortra. He has spent the last decade as a consumer of various data protection products and services. He is also a subject matter expert for global data privacy and compliance regulations. Wade applies this experience and knowledge when working with customers to understand and solve their real-world data protection use cases.

The Minds Behind the Insights

Christian Toon

Founder & Principal Security Strategist, Alvearium Associates

Christian Toon

Founder & Principal Security Strategist, Alvearium Associates

Christian Toon is a globally recognized expert in security and technology leadership, with over 17 years of experience driving strategic initiatives across a wide range of sectors. His extensive career has spanned senior executive roles in major corporations, government advisory positions, and board memberships. Christian is also a passionate and proven champion for inclusion and diversity within the security and technology fields.

The Minds Behind the Insights

John Grancarich

Chief Strategy Officer, at Fortra

John Grancarich

Chief Strategy Officer, at Fortra

John Grancarich, Fortra's Chief Strategy Officer, is driving the company's transformation into a global cybersecurity leader. With deep expertise in technology markets and operations, he focuses on innovation and advocates for using AI and automation to empower existing cybersecurity talent. Before joining Fortra in 2018, John founded Product Fuse and held senior roles at KLDiscovery, Kroll Ontrack, and Paul Hastings. He holds a bachelor's degree in Finance from Saint John's University and co-authored Internet Fraud Casebook: The Worldwide Web of Deceit.

The Minds Behind the Insights

Funso Richard

Publisher of Business Risk Pulse

Funso Richard

Publisher of Business Risk Pulse

Funso Richard is a distinguished Thought Leader and Executive Cybersecurity & Governance, Risk, & Compliance Advisor with over 15 years of experience in building robust cybersecurity programs. His profound expertise in leveraging cybersecurity strategies to mitigate business risks and enhance organizational value has made him a trusted advisor in the industry. As the publisher of Business Risk Pulse, he provides invaluable insights and thought leadership to business executives, helping them navigate the complexities of today's digital landscape. His prior tenure as Assistant Vice President of Cybersecurity at a leading US Healthcare Revenue Cycle Management Company highlights his exceptional ability to protect organizations against evolving cyber threats. His commitment to excellence and his strategic approach to cybersecurity have earned him a reputation as a visionary leader dedicated to safeguarding the digital future.

The Minds Behind the Insights

Dr. Muhammad Malik

Seasoned Information Security Leader

Dr. Muhammad Malik

Seasoned Information Security Leader

Dr. Muhammad Malik is a seasoned information security leader with over 25 years of experience, specializing in setting up security strategies and running comprehensive security programs. Currently leading the Information Security Program at a prominent media group in Qatar, he has a proven track record of enhancing security postures for both Australian government agencies and global enterprises.

His expertise spans corporate IT, broadcasting technologies, battlespace communication, and IoT environments. Dr. Malik holds a PhD in Computer Science from UNSW, and his credentials include CISM, CISA, CISSP, SABSA Foundation, and SANS GIAC Strategic Planning (GSTRT). Recently admitted to the Carnegie Mellon CISO program, he is also a frequent contributor to ISACA journals and a speaker at industry conferences.

The Minds Behind the Insights

Dimitris Georgiou

Chief Security Officer and Partner at Alphabit Cybersecurity

Dimitris Georgiou

Chief Security Officer and Partner at Alphabit Cybersecurity

Dimitris Georgiu started early in computing, and this grew into a strong professional interest, leading to years of fulfilling professional experiences in IT, Cybersecurity, and Consulting. After shifting his academic path, he gained experience employed or working as a contractor on a diverse set of projects for various industries. He is currently Chief Security Officer and Partner at Alphabit Cybersecurity in Athens, Greece, mostly working on cybersecurity consulting and digital forensics projects; Member of ISC2 Europe Advisory Council and second term Treasurer at ISC2 Hellenic Chapter.

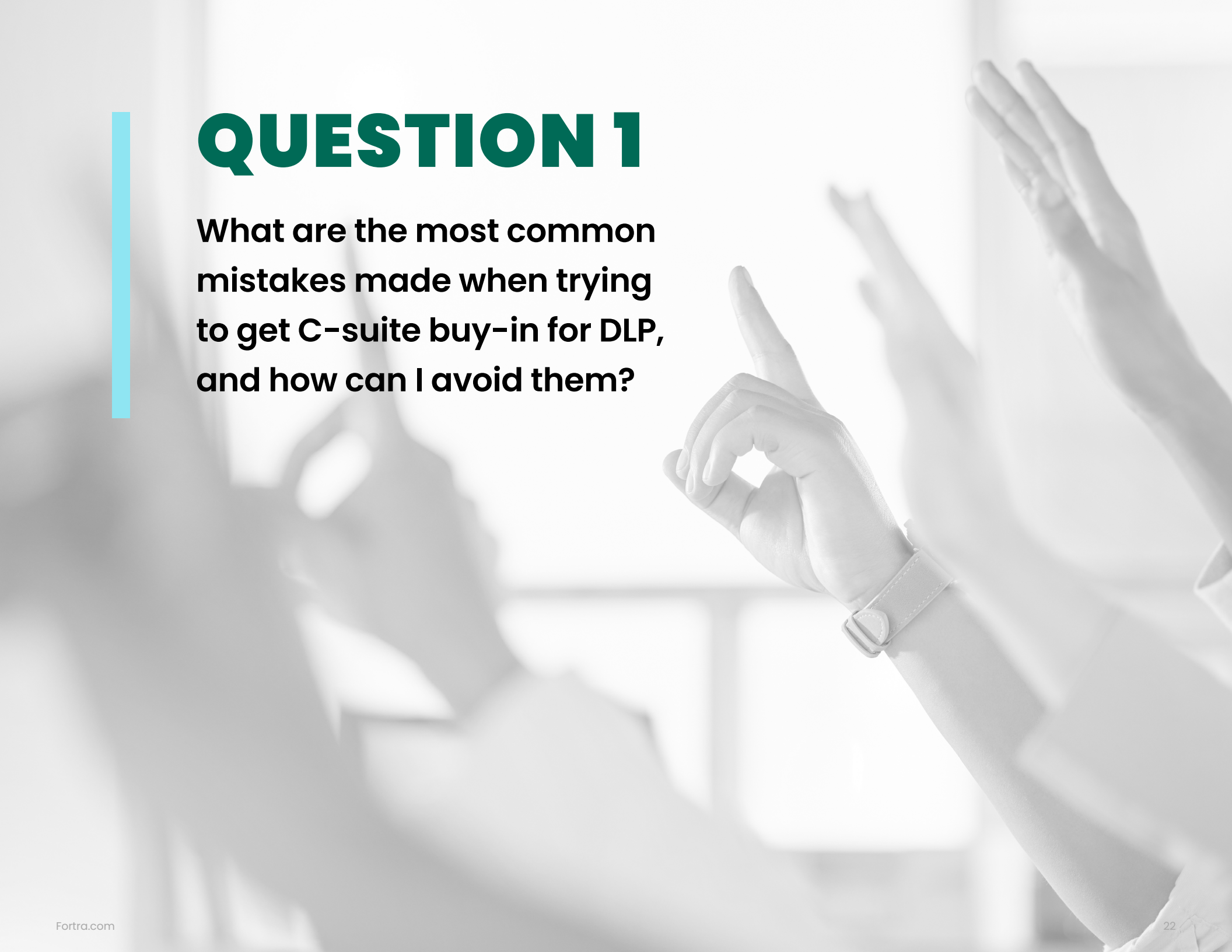
SECTION 1

Clearing up the Misconceptions

DLP is often perceived incorrectly. Whether it is the inability to calculate its protective value or its image as an evil overlord, the job of the security professional is to dispel the myths and offer clear information and expectations about the benefits to the organization.

QUESTION 1

What are the most common mistakes made when trying to get C-suite buy-in for DLP, and how can I avoid them?



Clearing up the Misconceptions

Ross Moore
Cyber Security Support Analyst with Passageways

Expense is always top-of-mind, and rightly so. "Expensive" gets thrown around a lot in all departments. What does expensive mean? It often connotes the benefits of the projected result being outweighed by the cost of attaining that result. We all examine ROI calculations all the time with things like insurance. I may pay a particular amount regularly, but if it saves me from paying more, then it's considered a good deal. Even if something is perceived as expensive, we still pay for the potential benefits.

It's hard to forecast ROI with security and privacy. Security and privacy are often seen as preventive measures, in which case they don't earn money; they keep companies from paying penalties. Calculating that is like proving a negative - when nothing bad happens, was it because of the protections or because, in truth, nothing happened? If something had happened, would it have been so bad after all?

While there's plenty of data in the wild, there's also a lot that isn't out there, including new customers' data (consider them "information assets") that has been entered after any previous compromises. Companies don't need to be part of an ecosystem that is willing to let its guard down and provide more free data to fill the dark web markets in perpetuity.

For DLP, a major calculation that can be overlooked is: what's the cost if the risk materializes versus what would it cost to prevent or mitigate it, e.g., What would it cost a healthcare provider if 100,000 medical records were stolen? What would it cost a fintech company if thousands of payment card records were exfiltrated and sold? What if 10K clients of a law firm had their intellectual property stolen?

Clearing up the Misconceptions

Ross Moore

Cyber Security Support Analyst with Passageways

It's important to estimate the total costs of stolen data - legal fees, lost revenue, class action lawsuits, and company resources spent in restoration and recovery, hiking up the total. Now, compare that to the cost of a DLP solution.

Having a reputation for data protection actually plays a direct part in revenue because it raises the credibility and reputation of an organization, so a customer is more likely to pick a reputable company, especially if the services and costs are similar.

Dr. Alea Fairchild

Research Fellow at The Constantia Institute

C-suite executives often have several common misconceptions about DLP. One of these is that DLP is solely an IT problem, overlooking the need for organizational policies, employee training, and a comprehensive data governance strategy.

There is also a belief that DLP measures will hinder employee productivity. In fact, with the right implementation, DLP can enhance security without significantly disrupting workflows, especially when assisted by causal AI and machine learning.

DLP requires a combination of technology, processes, and people to be truly effective. It helps for buy-in to have clear metrics for risk assessments that quantify the potential risks of data loss and how DLP can mitigate these risks.

Clearing up the Misconceptions

Wade Barisoff
Director, Product Management, Data Protection, at Fortra

DLP is treated as a threat prevention tool. However, it is more of a compliance and regulatory tool with some threat prevention overtones. Companies naturally place it in Cyber Defense, and it is run and maintained by the threat teams that then want to treat it as a threat tool only. Since threat prevention is a tiny percentage of what DLP does, it is very hard to justify the value, and eventually, there are discussions of "do we need it" or "how cheap can we do it," which leads a company to be exposed in some way (since threat prevention is such a tiny portion of what DLP catches).

To have a successful DLP implementation is a partnership between business and cyber security teams, and the privacy/ legal/compliance teams are the business customers of the team running it. DLP is the electronic enforcement of corporate policy for data handling. When you do that, will you catch someone sending data inappropriately, possibly even stealing data? For sure, but that is arguably a minimal occurrence, despite what some vendors would like you to believe.

Most of what DLP does is education. It catches violations of corporate policy or bad practice.

Clearing up the Misconceptions

Christian Toon
Founder & Principal Security Strategist, Alvearium Associates

In my two decades of leading security teams and building control frameworks, I've observed that the term "data loss prevention" often creates unrealistic expectations. In reality, we should think of it more as "data loss minimization," recognizing that some level of data leakage is almost inevitable. Even in high-security environments like national intelligence agencies, human error or deliberate actions lead to data breaches.

When approaching C-suite executives about implementing robust data protection measures, it's crucial to dispel common misconceptions. Many executives view data protection as solely an IT issue, failing to recognize its broader business implications and impacts on non-digital information. They may also underestimate the ongoing nature of effective data security, mistakenly believing it's a one-time implementation rather than a continual process.

Clearing up the Misconceptions

John Grancarich

Chief Strategy Officer, at Fortra

A common concern I hear about relates to the potential for DLP to reduce end-user productivity and hinder overall business operations. The reality is that modern DLP solutions are designed to be minimally invasive, provided that they have been properly configured during the initial implementation. If a DLP solution is causing disruptions, it's often because policies are too restrictive or not well implemented. Tailoring policies to fit specific business needs can mitigate this concern.

Additionally, I have sometimes seen instances where executives believe that DLP is a "set it and forget it" type solution, but the reality is that similar to other security solutions, it requires continuous monitoring, updates, and policy tuning. Since things are always evolving, such as threats and business processes, ongoing tuning and adaptation will be an ongoing need as well.

Funso Richard

Publisher of Business Risk Pulse

Many C-suite executives mistakenly view DLP as a one-time technical solution that will solve data breaches, overlooking its integration with broader security strategies. They also assume DLP solutions are one-size-fits-all, ignoring the need for customization to meet specific organizational needs and compliance requirements. These misconceptions can create gaps in data protection and a false sense of security.

Clearing up the Misconceptions

Dr. Muhammad Malik
Seasoned Information Security Leader

C-suite executives often have several misconceptions about DLP solutions, which can lead to strategic missteps or under-utilization. Among the most common are:

- **DLP as a Simple Tool, Not a Program:** Many executives mistakenly view DLP as a one-size-fits-all tool, expecting a quick fix rather than recognizing it as a comprehensive program that requires policy integration, trained staff, and ongoing updates to be effective.

- **Productivity Concerns:** There is a common belief that DLP disrupts productivity. Modern DLP solutions, however, are highly customizable, enabling minimal disruption by allowing tailored data access levels and workflow integration.

- **Overlooking Privacy Regulations:** There is a tendency to underestimate the complexities of regional privacy laws. A one-size-fits-all DLP deployment can lead to compliance risks, especially in stringent regions like the EU, where a phased, region-specific approach is essential.

- **Expecting Immediate Results: Executives often anticipate rapid, large-scale results. However, successful DLP programs should start with focused, high-impact use cases to build momentum, avoiding overwhelm and allowing iterative improvements over time.**

These insights emphasize the need for DLP as a strategic, flexible program—aligned with both organizational needs and regulatory compliance—that matures and adapts over time for maximum effectiveness.

Clearing up the Misconceptions

Dimitris Georgiou
Chief Security Officer and Partner at Alphabit Cybersecurity

DLP often faces misconceptions at the executive level, primarily around its nature and purpose. One key misunderstanding is viewing DLP solely as a technical fix rather than a strategic, ongoing initiative. C-suite leaders sometimes perceive DLP as a simple tool that, once installed, handles itself. In reality, effective DLP requires continuous monitoring, policy adaptation, and, crucially, employee engagement.

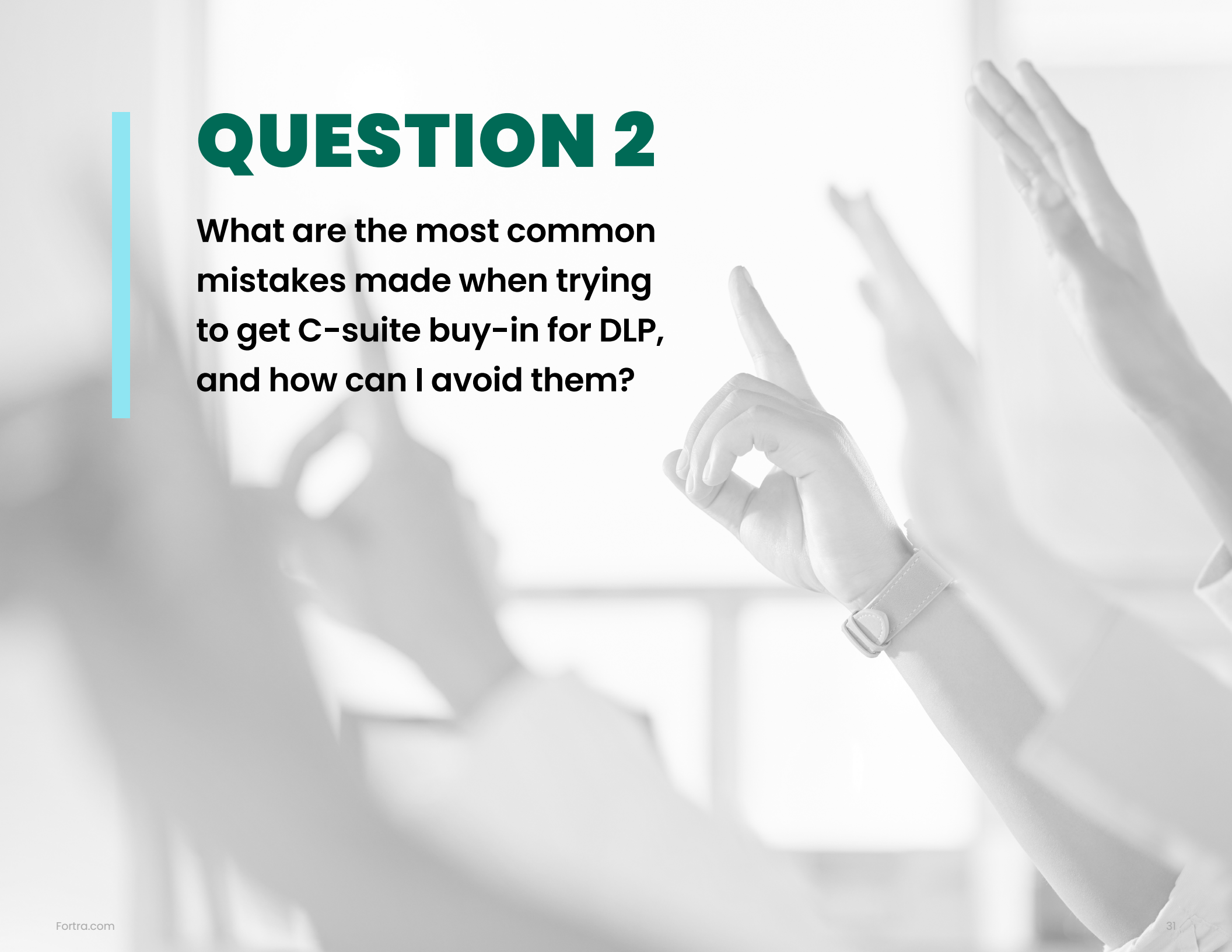
SECTION 2

Speaking the Language of Business

One of the problems that often occur when a technology professional walks into the Board Room is the wrong use of language. While it's important to establish oneself as an expert in a particular discipline, it is equally important to recognize that the company already knows that. The new challenge is to expand upon the technical acumen and demonstrate business acumen. Our experts clarify what it means to "speak the language of the business".

QUESTION 2

What are the most common mistakes made when trying to get C-suite buy-in for DLP, and how can I avoid them?



Speaking the Language of Business

Ross Moore

Cyber Security Support Analyst with Passageways

One of the common mistakes is misunderstanding the security philosophy of the C-suite. Is spending geared to get a positive attestation or assessment report that looks good on the marketing website, or is it to protect data? When that's discovered, a proper case can be made.

Attestations and clean assessment reports are definitely worth it in and of themselves because they demonstrate adherence to a security baseline, and having a DLP solution is part of maintaining regulatory compliance in many cases.

If the security approach is part of a larger initiative of "we'll do our utmost to keep your data secure, though it will take time," then DLP will play a larger part in the security strategy.

Dr. Alea Fairchild

Research Fellow at The Constantia Institute

One of the common mistakes that many technical folks make is speaking only from the technology perspective when presenting the needs to the C-suite. It's not that the executives don't understand the technology. These days, many of them have more technical knowledge than previous generations. However, **when presenting a business case, the focus must be on what the solution brings to the business. In the case of DLP, the central point is that it gives the company better control of their important data. This is what is meant when people advise technologists to "speak the language of the executives."**

Speaking the Language of Business

Wade Barisoff

Director, Product Management, Data Protection, at Fortra

Too often, the person seeking buy-in tries to sell it as a threat tool, but the collected data needs to be carefully analyzed to prove all the threats it is catching to justify the cost. I've seen outlandish scenarios presented, too, that try to scare the budget out of C-suite executives, which will always backfire, as you then need to find a bad actor, which is rare.

The CISO should never solely try to justify DLP, as it should be a partnership between the CISO, legal, privacy, and compliance teams. In the case of manufacturing, the individuals in the company responsible for research and design need to be included as well since company intellectual property is paramount in some manufacturers. If you think about that approach, one person (the CISO) justifying the need, or potentially four voices justifying the need, it becomes much more powerful as a team.

Christian Toon

Founder & Principal Security Strategist, Alvearium Associates

To gain executive buy-in, it's essential to frame data protection in terms of business risk and potential financial impact. This means moving away from technical jargon and instead focusing on how data loss minimization supports overall business objectives, including maintaining customer trust, ensuring regulatory compliance, and preserving competitive advantage.

Quantifying potential losses from data breaches – including regulatory fines, legal costs, R&D costs, and reputational damage – can be particularly effective in capturing C-suite attention. Mistakes also stem from how it's positioned; it's better to present it as a business protective control rather than a totalitarian monitoring tool.

Speaking the Language of Business

John Grancarich

Chief Strategy Officer, at Fortra

It's critical to know your audience, what they care about, and what concerns them so that you can design a strategy that speaks to those needs and finds a mutually agreeable path forward. Sometimes, DLP is presented as purely a security or compliance tool with little connection to broader business objectives. This can make it seem like an IT issue rather than a company-wide priority.

Additionally, some executives will be focused on growth, while others may prioritize operational efficiency, cost-cutting, or regulatory compliance – it's important to understand the playing field you're operating on so that you can work toward gaining alignment and establishing a unified path forward. Connect with those leaders one-on-one and develop a clear understanding of what they each care about, then work to put it all together into a cohesive plan to achieve buy-in.

Funso Richard

Publisher of Business Risk Pulse

A common mistake in securing C-suite buy-in for DLP is not aligning the proposal with business objectives. Advocates often focus too much on technical details and threats without showing how DLP supports strategic goals and protects critical assets. To avoid this, it's important to present DLP as a business enabler, highlighting its role in safeguarding intellectual property, ensuring compliance, and maintaining customer trust.

Additionally, **using clear, non-technical language and providing concrete examples of financial and reputational impacts can bridge the gap between technical and executive perspectives, making the case for DLP more compelling.**

Speaking the Language of Business

Dr. Muhammad Malik
Seasoned Information Security Leader

Securing C-suite buy-in for DLP solutions requires bridging the gap between technical details and business goals. A common mistake is presenting DLP as a purely technical project rather than a strategic business enabler. Executives respond better when DLP is clearly tied to strategic initiatives, demonstrating how it protects the organization's goals, reputation, and financial stability. Positioning DLP as a tool that enhances business priorities becomes integral to achieving broader company objectives rather than an isolated IT initiative.

Other common mistakes include failing to align DLP with business initiatives, focusing too much on features instead of value, and not integrating it with existing risk frameworks. Providing clear ROI, involving business leaders from the start, and avoiding overly technical language is key to successful buy-in. **Effectively pitching DLP to executives means framing it as a business-aligned, value-driven solution that addresses organizational risks and supports strategic goals.**

Speaking the Language of Business

Dimitris Georgiou
Chief Security Officer and Partner at Alphabit Cybersecurity

A frequent mistake in securing executive buy-in for DLP is emphasizing technical specifics over business impact. While the details are essential to IT, executives are more interested in how DLP mitigates risks, enhances compliance, and protects the company's reputation. Security professionals often miss the mark by not illustrating DLP's direct business value.

Another common error is overlooking ROI. Leaders tend to view security investments as cost centers, so highlighting how DLP prevents costly breaches or compliance fines can be critical. For example, citing industry-specific breach costs and potential savings from avoiding penalties or data loss can make DLP's financial value clearer.

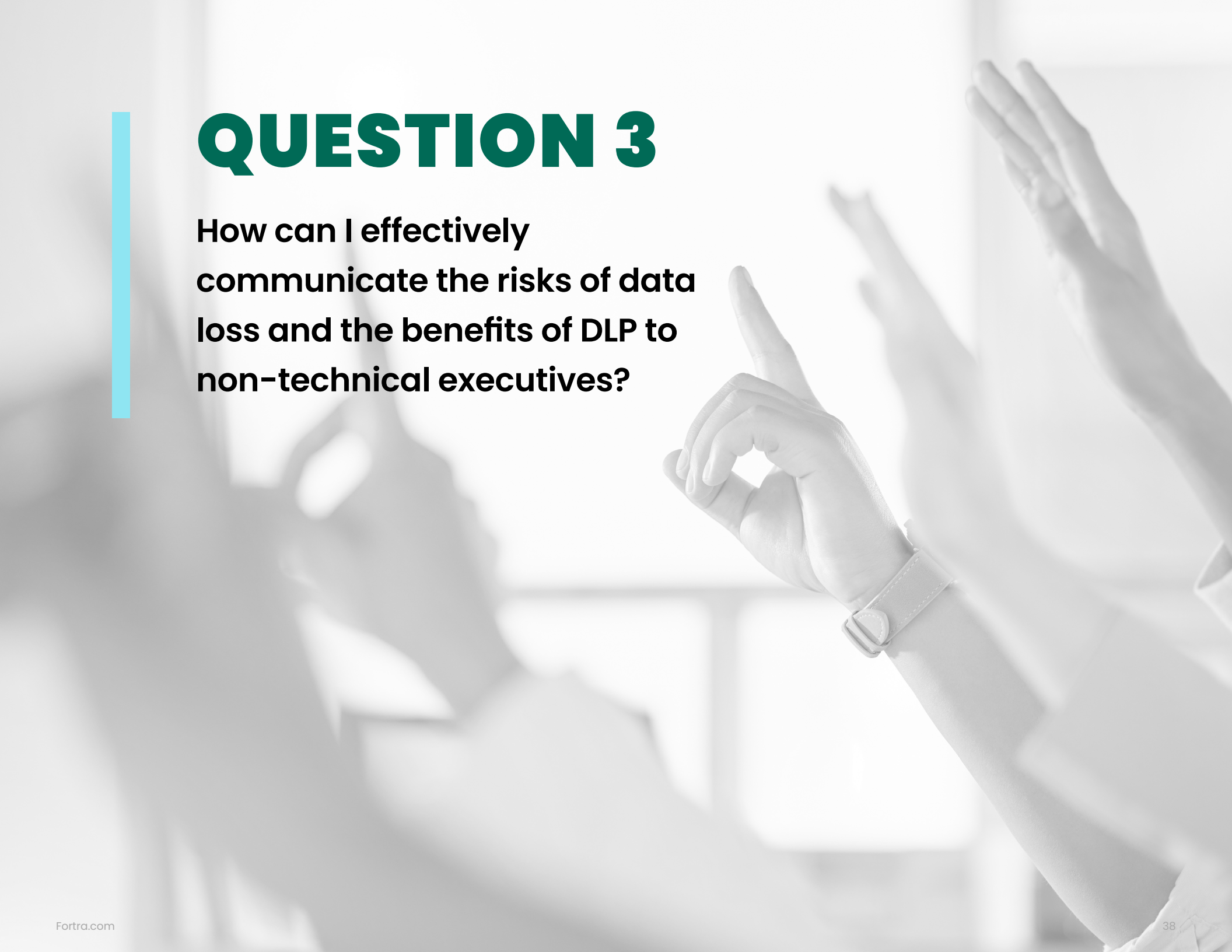
SECTION 3

Communicating Risk

It is important to communicate risk without making it seem like the company will go out of business at every discovery of a problem. Similarly, the benefits of a security solution must be tempered against overselling it as the solution to all the risks.

QUESTION 3

How can I effectively communicate the risks of data loss and the benefits of DLP to non-technical executives?



Communicating Risk

Ross Moore
Cyber Security Support Analyst with Passageways

Don't expect executives to be highly technical. Many of them are technical, and many of them are not, and that's OK - they have plenty of other business aspects to manage. They're expecting their security experts to transfer the message in a relevant way, which usually involves numbers and graphs. At least be able to show numbers of "we spend $X to avoid costs of $X, Y, and Z".

Along with the financial analysis, part of maintaining attestations and clean reports is being able to demonstrate that rules and alerts are configured correctly so appropriate action can be taken when certain data is suspected of being accessed by unauthorized individuals. **DLP plays a major role in compliance by having an additional layer of visibility into who's doing what with the data.**

That compliance leads to sales because customer expectations of those attestations have set the bar. The message can be, "Because we spent money on compliance initiatives, we received tenfold in new sales this year." Or even, "Because we didn't have particular certifications, last year we missed out on numerous sales that would have more than covered the cost of the certification."

Communicating Risk

Dr. Alea Fairchild

Research Fellow at
The Constantia Institute

Some effective ways of communicating the risks include sharing case studies or news stories about recent data breaches and focusing on the financial, reputational, and operational impacts on organizations similar to your specific organization or industry. Emphasize how data loss can affect revenue, customer trust, and regulatory compliance. **Illustrate the potential costs of a breach compared to the investment in DLP solutions. Explain how using DLP creates mechanisms to meet legal and regulatory obligations, reducing the risk of fines and legal issues.**

Wade Barisoff

Director, Product Management,
Data Protection, at Fortra

When I worked directly with the CTO of a Fortune 4 company, I was tasked with showing him and the other executives what we had done with our program. I was presenting to the CISO, the Chief Privacy Officer, and our head of the legal team. I showed them three bad business processes that were in operation and what regulations we were violating. The violations were corrected, and the CPO indicated how we avoided possible fines.

We also reported that we had cleaned up over 400 million files that no longer had material value to the company. The legal representative shared that retaining those files presented a liability risk if we had to perform discovery; that data could be harmful to the company. Surprisingly, we caught a person who was trying to exfiltrate data to a spouse who was in jail for identity theft.

Communicating Risk

Wade Barisoff

Director, Product Management, Data Protection, at Fortra

Your partners justify the need and the risk for you, and the CISO should never be the only person held responsible in the organization. Many times, when partnering with your business partners, your scope is reduced, focused, and only impacts business processes that do not follow company policy. Without DLP, you would never have found and corrected those practices until a breach had been caught by someone and escalated to executive level. This is the difference between a panic and scramble for DLP versus a thoughtful implementation.

Christian Toon

Founder & Principal Security Strategist, Alvearium Associates

One of the most impactful ways to communicate the importance of data protection is through real-world examples and case studies. I've found that relatable analogies and visual aids like infographics can help non-technical executives grasp complex concepts more easily. It's also crucial to involve key stakeholders from various departments early in the process, ensuring a comprehensive approach that considers not just technology but also processes and people.

Communicating Risk

John Grancarich

Chief Strategy Officer, at Fortra

To be effective when communicating the risks and benefits, it is vitally important to know your audience and what they care most about. For some leaders, it will come back to things like the potential for lost revenue, impacts on customer trust, and competitive disadvantages. It's important to know which matters the most so that you can frame the conversation accordingly.

I also like to quantify the cost versus benefit wherever possible. Put it into a language they can then use to communicate with others. For example, if we use the common metric of a data breach costing an organization over $4 million per incident, we could credibly claim that for a fraction of the cost of a typical breach, we can implement a modern DLP solution to proactively head off a material risk like this.

Funso Richard

Publisher of Business Risk Pulse

To effectively communicate the risks of data loss and the benefits of DLP to non-technical executives, stakeholders should use relatable scenarios and case studies. These instances should illustrate how data breaches have negatively impacted similar organizations. They should also highlight how DLP solutions can proactively prevent such incidents by protecting sensitive information, enhancing business resilience, and building trust with customers and shareholders.

Communicating Risk

Dr. Muhammad Malik
Seasoned Information Security Leader

To effectively communicate the risks of data loss and the benefits of DLP to non-technical executives, it's crucial to frame DLP as a strategic enabler rather than just a control measure. Present it as a proactive initiative that supports the business in achieving its core objectives by safeguarding reputation, ensuring regulatory compliance, and building customer trust—all essential for sustainable growth. Position DLP as a key asset that enhances operational resilience enabling the company to pursue digital initiatives and innovation confidently without compromising data integrity.

Use relatable scenarios to illustrate DLP's role in facilitating business agility. For example, demonstrate how DLP enables secure data usage in emerging markets or under strict regulatory frameworks, thereby opening doors for expansion and increased customer engagement.

Instead of focusing on technical details, emphasize DLP's value in protecting strategic assets and enhancing decision-making. This empowers the organization to take calculated risks and seize opportunities with data assurance in place. By showcasing DLP as an investment in both growth and resilience, you clarify its value in terms that executives care about most.

Communicating Risk

Dimitris Georgiou
Chief Security Officer and Partner at Alphabit Cybersecurity

To make a compelling case, I focus on risk management and business resilience. Rather than diving into technical specifics, I present "what if" scenarios - what if a competitor accessed proprietary data or if customer data were compromised? Grounding these risks in familiar business impacts - reputational damage, regulatory penalties, and lost revenue - often resonates strongly with non-technical leaders.

Positioning DLP as part of a unified cybersecurity strategy rather than a standalone tool also strengthens its appeal. An integrated approach, combining DLP with threat detection and access control, not only optimizes security but presents a streamlined, strategic solution that executives tend to appreciate.

SECTION 4

Telling a Story

Few examples better illustrate the value of an initiative than a real-world scenario. We are receptive to stories and experiences. Our experts shared some of their more memorable moments where DLP was instrumental in protecting the organization.

QUESTION 4

Tell me about a real-world scenario where DLP played a critical role in preventing a potential issue.

Telling a Story

Wade Barisoff

Director, Product Management, Data Protection, at Fortra

One time, we generated 10,000 events in a short time. Looking at the data, we could see that legitimate blocks were occurring as there was a customer social security number in plain text e-mail. Looking through the data, we could see they were system-generated e-mails.

We found that a development team had just launched a new system with automated customer correspondence and made a mistake, including the SSN from the consumer database in the outbound e-mail. That was quickly corrected, and the system was back online and in compliance.

There was an individual who would always generate dozens of DLP events a day in our system. Our team reached out and educated the individual that their messages were not being sent and the warning message generated by the DLP system was legitimate.

This continued, so we reached out to the individual's manager and found out they had made up their own business process and were not following the standards of the organization. DLP prevented the violation that would have compromised the business.

In another instance, I received a call from one of my team members who said that a company VP was seriously displeased with the DLP system and wanted to talk to me. The VP proceeded to yell at me about how our system was stopping him from communicating the quarterly progress of his program to his external partners like he had done a half dozen times already.

I asked what he was sending that was getting blocked, and he told me it was a PowerPoint presentation that they had used before. I asked if he could share it, and as we flipped through the slides, there was a graph on page three. I asked him to right-click and show the Excel file behind that graph, and out popped an Excel file filled with consumer information, including medical data and Social Security number (SSN) information.

The person who created the graph forgot to strip the unnecessary columns from the spreadsheet and was about to violate privacy law. He quickly apologized and said they would get the mistake corrected.

Telling a Story

Christian Toon

Founder & Principal Security Strategist, Alvearium Associates

In my experience, successful data protection initiatives often reveal unexpected benefits. For instance, I once worked with a company where a well-implemented system not only prevented a significant data leak but also helped identify gaps in security awareness training and procedural gaps. This led to improved overall security measures and a more security-conscious culture throughout the organization.

John Grancarich

Chief Strategy Officer, at Fortra

We have a large number of customers using our DLP solution and naturally hear about various types of use cases and situations they encounter. Something we hear about more than you might think is human error. While there are instances of bad actors attempting to do bad things that we block, it's interesting to see how the inadvertent inclusion of an unintended email address to an email can happen or how an additional file can be selected for upload to a file-sharing site. Sometimes, the interesting things are simply part of the ordinary work we all try to do each day.

Telling a Story

Funso Richard

Publisher of Business Risk Pulse

I remember a scenario where DLP prevented a data incident. Our organization had DLP policies to monitor data sharing on virtual desktops. An employee inadvertently tried to download sensitive data from a virtual desktop to a physical computer. The DLP system flagged and blocked the attempt, alerting our security team. This incident highlighted DLP's crucial role in preventing data exfiltration and ensuring compliance.

Dimitris Georgiou

Chief Security Officer and Partner at Alphabit Cybersecurity

A notable instance in my career illustrated DLP's impact when unusual data transfer activity was detected with a customer on an employee's account. Further investigation revealed an insider attempting to export sensitive information, potentially causing significant loss and reputational harm. This incident underscored the importance of DLP as a safeguard against both external and internal threats, reinforcing the value of early detection.

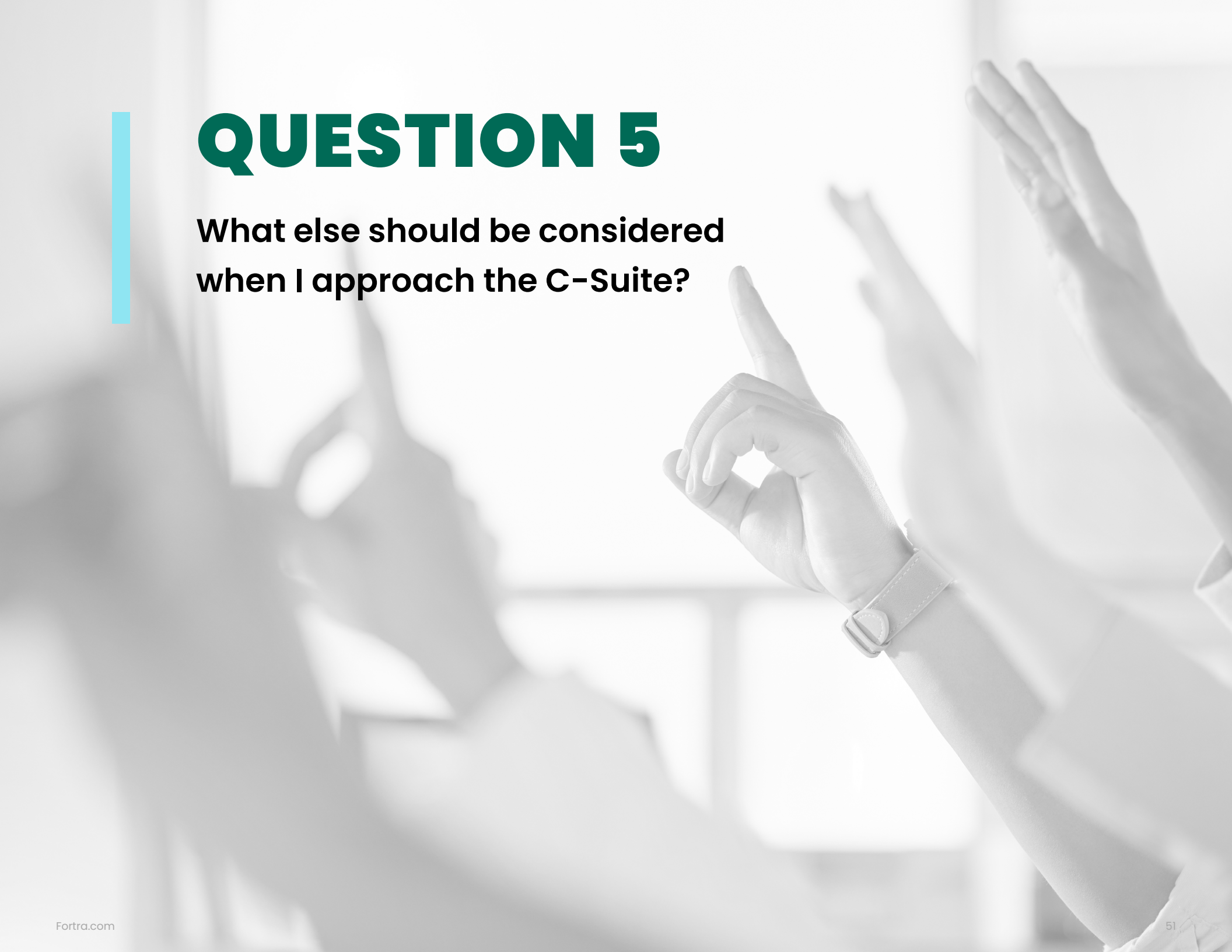
SECTION 5

Making it Happen

Approaching the C-Suite about DLP implementation can be a step into the unknown. Our experts were eager to express some words of optimistic encouragement for any security professional who is working to gain approval for a DLP solution.

QUESTION 5

What else should be considered when I approach the C-Suite?



Making it Happen

Ross Moore
Cyber Security Support Analyst with Passageways

Remain a business professional. For security practitioners, it's easy to side more with the practitioner role than the business and employee roles. Try to get an understanding of the corporate priorities and financials (even just an overview) so you can better articulate where DLP might fit in the overall milieu and when in the year to present it. Perhaps frame it more as "protection" than "prevention." Some may perceive prevention as too close to a “magic elixir.” Get to know your company culture and lingo.

Look inside and shop around. Some questions to consider include: Are there any options in your tech stack already that might do just fine? Are there add-ons to your current technology that present a low-cost entry? What kind of DLP solution do you need? Work to find a reasonable angle for your presentation.

Don't try to sneak it in. It needs to be an open part of the whole security, privacy, and compliance conversation. With DLP being one piece of the whole layered security puzzle, don't present it as the one solution to rule them all. Let the C-suite know that you've done your due diligence in placing DLP in its proper place in the schema.

Point out what the DLP product actually does. Be succinct and clear about how it protects and how it doesn't protect. Present more than one choice, either selecting different vendors or different tiers of a product. You may not get the top-shelf vendor or product, but the leaders may choose one of your other options. We may have a preference as individuals, but from a security professional perspective, even what we might consider a lesser choice is still a solution. Take the wins at whatever level you can.

Making it Happen

Wade Barisoff
Director, Product Management, Data Protection, at Fortra

Data loss prevention programs require thoughtful partnership and focus on enforcing policies that will ensure the company does not need to deal with accidental loss and the occasional malicious insider.

If it is treated as a transient or a “part-time” effort, DLP will cause disruption to the company and business workflows as it is not a threat tool. Threat tools you drop in, do some basic configuration, and they monitor/compare inbound traffic to rules pre-defined by the vendor to find malicious threats. The team responsible simply needs to understand the output of the tool and any remediation actions they need to take.

DLP is a blank slate that requires an understanding of the business, what needs to be monitored, and what the most efficient way to monitor that data is. DLP products come with pre-defined rules, but it is the combination of those rules that make it effective. **A team that is invested in understanding your company's corporate policies on handling data, what rules the DLP tool offers that help them find that data, then partnering with Legal, Privacy, and Compliance on how to handle the inspection and what actions should be taken are the foundations of any good DLP program.**

DLP programs only need to disrupt bad business practices; that is its purpose. There are many poor implementations of DLP that lacked a plan or a program wrapped around it, which impacted business workflows negatively and caused the C-Suite to question the value of such a product.

Making it Happen

Wade Barisoff
Director, Product Management, Data Protection, at Fortra

Key items to successful implementation are quite simple:

- Create a plan, listing what you are going to protect.
- Show the steps you are going to take to ensure you are not going to disrupt good business workflows. (This means showing how you are going to monitor what DLP is doing, tuning the rules to ignore good practices, and what bad practices were found during the monitoring period).
- Have your business partners (Legal, Privacy, Compliance, R&D) advocate how important the program is to the profitability and reputation of the company.

A thoughtful approach that includes your business partners is how any DLP program will be successful. Those leaders need to advocate for the program and explain how important it is for the company to have these guardrails in place to ensure your customer data or company intellectual property is not accidentally lost. Those losses can impact a company in very insignificant ways to public fines and large impacts on profitability.

Making it Happen

Christian Toon

Founder & Principal Security Strategist, Alvearium Associates

Ultimately, the key to successful DLP implementation lies in fostering a culture of continuous improvement and adaptation. It's more than just the technology. While the initial investment may seem significant, the long-term benefits of protecting sensitive data far outweigh the costs of potential breaches or non-compliance. By presenting a clear ROI model that includes both tangible and intangible benefits, you can help executives understand that effective data protection is not just a security measure but a crucial component of overall business strategy in our increasingly data-driven world. Also, the rise in AI DLP Security is breathtaking - really set to disrupt the traditional DLP markets. A great time to get in on some innovative technology at a good price.

John Grancarich

Chief Strategy Officer, at Fortra

Step your way through the process and build alignment at each step of the journey. **Realize that you are not selling a technical solution as much as a business outcome,** so be sure to learn the language of the business people and what they care about, and then speak that language. Listen, learn, and think carefully before putting a proposal on the table and asking for a commitment or an investment. **Not only will you likely have better success, but you'll also build trust, which is the foundation for all the progress you'll be able to make.**

Making it Happen

Funso Richard

Publisher of Business Risk Pulse

When seeking C-suite buy-in for DLP solutions, it's crucial to demonstrate a clear ROI. Professionals should emphasize cost savings by preventing data breaches, avoiding fines, and protecting the company's reputation. They should also highlight how DLP enhances operational efficiency by automating data protection and reducing IT workload.

Dr. Muhammad Malik

Seasoned Information Security Leader

Effective stakeholder management is critical. Using a structured approach like SIPOC (Suppliers, Inputs, Processes, Outputs, Customers) enables a comprehensive understanding of stakeholder needs and expectations. This approach helps to map out key “suppliers” of relevant information (such as compliance, IT, and risk teams), the “inputs” necessary for the DLP solution (including data protection policies and resources), the “processes” involved in DLP implementation, and the intended “outputs” (such as enhanced data security and compliance). By clearly identifying the “customers” or end beneficiaries—executives and business units—you can better align the DLP initiative with stakeholders’ objectives and expectations.

Making it Happen

Dr. Muhammad Malik

Seasoned Information Security Leader

Beyond this mapping, successful stakeholder management involves proactive communication to demonstrate DLP's relevance to core business needs. Engage stakeholders by illustrating how DLP mitigates specific business risks, such as regulatory breaches or reputational damage, using real-world scenarios that resonate with their priorities. For example, linking DLP outcomes to financial stability or customer trust can help non-technical stakeholders see its strategic value. In managing these relationships, it's essential to tailor language and data to each stakeholder group, focusing on how DLP supports their roles and overall company goals, ensuring that they view the solution as a strategic asset rather than a technical expense.

Dimitris Georgiou

Chief Security Officer and Partner at Alphabit Cybersecurity

Ultimately, securing buy-in for DLP requires positioning it as a strategic priority that supports broader business goals - protecting data, maintaining trust, and ensuring compliance. By framing DLP in terms of these core business objectives, security professionals can foster executive support and highlight DLP's role in strengthening organizational resilience.

Conclusion

DLP is an important part of a data protection program. However, since a DLP solution touches everyone in an organization in a very personal way, it is important to work with all departments to make its deployment successful. The tips and sentiments offered by our experts should ease the discussions and lead to a positive outcome, not just for the implementation of a security product but for the security of the organization that you protect.

Further Resources

Fortra offers a range of resources to deepen your understanding of data loss protection. Explore Digital Guardian's Definitive Guide to Data Loss Prevention for an in-depth look at strategies and tools to protect sensitive information across your organization. Our dedicated resources page provides a wealth of insight for those wanting to understand more about DLP, including webinars, datasheets, whitepapers, and blogs.

To request a Digital Guardian demo, Contact Us!

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-corp-ebook-1224-r1-an