TANIUM

CHIEF DISRUPTOR

Information Risk Management – Expectations Versus Reality

A Tanium *Point of View* report in partnership with Chief Disruptor.

POINT OF VIEW REPORT

CONTENTS

Introduction

Information and security management have often been measured in terms of costs incurred, instead of business outcomes achieved. This is changing as uncertain operating conditions for businesses mean commercial growth is increasingly tied to an accurate understanding of risk. But digital transformation presents new challenges for organisations that want to gain a clearer view of their IT assets, technology risks and vulnerabilities.

> "Cybersecurity is a top three risk. We recognise that as a leadership team and as a company, so it will feature quite significantly in 2023."
>
> **Chief Information and Security Officer**
> FTSE 100 packaging business

To address this challenge, senior leaders are developing new strategies to embed information risk management into the fabric of how they do business. Amid this change, we wanted to uncover whether gaps still exist between the ideation of these strategies and the actual maturity of their implementation.

In this report, we explore the contextual push and pull factors influencing the information and security sector's level of maturity. We then outline commonly referenced gaps between the expectation and the reality when it comes to information risk management. The report concludes with guiding principles to help close the expectation gap between strategy and implementation.

Acknowledgements

The authors thank the senior members of the Chief Disruptor community who gave their time to be interviewed for this report in the fourth quarter of 2022. Their views, some of which are quoted in the following pages, have guided the direction of this report. We are grateful for their invaluable contributions and insights.

Interviewees

- Erik Gaston, VP Executive Engagement, Tanium
- Zac Warren, Chief Security Advisor, Tanium
- Barry Panayi, Chief Data & Insight Officer, John Lewis
- James Tomkins, Chief Architect, Met Office
- Jon Roughley, Director of Data Strategy and Innovation, Experian
- Paul Curtis, Chief Technology Officer, Easyjet Holidays
- Matthew Wilmot, Group Head of Enterprise IT & Information Security, Fraser Group
- Chief Information and Security Officer, Government department
- Chief Information and Security Officer, FTSE 100 packaging business
- Senior Manager, CERT, Vodafone
- Que Tran, Regional Chief Information Officer, DP World
- Ketan Patel, Group Chief Information Officer, WH Smith

SECTION 1

The Current Landscape

The Changing Shape of IT

Our interviewees acknowledged there had been a rapid evolution in IT infrastructure in recent years. The switch from on-premises data centres to public and hybrid clouds has been a key disruptor. The move has brought about operational advantages including speed to market, scalability and the ability to gather and store more data.

From a security perspective, these developments have necessitated a new approach to information risk management. With physical on-premises storage, an organisation's technology assets are tangible and IT assets can be assessed with traditional approaches to inventory management.

With the proliferation of software and cloud solutions, the complexity of the IT landscape has exponentially increased. The move to remote working and the use of personal devices means the border of an organisation is no longer physically defined and the vectors of attack have expanded.

> "We have employees who want to use their own devices, or they may want to work in various locations around the world. All these factors add more complexity to the network."

Paul Curtis
Chief Technology Officer, Easyjet Holiday

> "It's not about securing a border that's maintained by a highly specialist team anymore because vectors of attack now include using Whatsapp or opening an email"

James Tomkins
Chief Architect, Met Office

As businesses are increasingly structurally underpinned by technology, a breach or an attack relates directly to a businesses' ability to operate, as well as to the customer experience and brand equity.

> "The risk did materialise about 3–4 years ago and we had a major data breach that was very public. It massively impacted our reputation. From there we invested in a risk management and cybersecurity programme."

Paul Curtis
Chief Technology Officer, Easyjet Holiday

The risks associated with the poor management of IT assets can lead to significant losses for a business. For every hour that a website is down, a business could be losing significant revenue. The charges and penalties associated with a breach are also noteworthy. Negative press coverage and social media discussions can also impact future revenues. With these factors in mind, the business case for investing in tools, processes and people to move beyond compliance towards cyber resilience becomes clear.

"Security is becoming a higher priority every year. There are more stories than ever before about companies that have had serious breaches. As a result, security solutions are winning the funding race because these are new risks and the outcomes could be catastrophic."

Barry Panayi
Chief Data & Insight Officer, John Lewis

> "Slow is like the new down. Your website doesn't have to be down for it to cause reputational damage. If it's slow you could end up with negative reviews on a social media feed."

Erik Gaston
VP Executive Engagement, Tanium

Many of our interviewees predicted that the dissolution of organisational boundaries will continue in 2023 and beyond. As businesses increasingly work in close collaboration with partners to overcome common challenges such as climate change, supply chain disruption and inflationary pressures, the need for businesses to share data and information beyond their organisational boundaries is growing. All this has created a compelling case for more prioritisation and investment into information management and security solutions.

"We've introduced standard protocols for how all our partner organisations come into our network and this reduces the risks we're carrying. This is as opposed to what we've done historically, which was to put something different together for each partner. Before you know it, you're managing many different systems just to manage data coming in and out," says Paul Curtis, the Chief Technology Officer, at Easyjet Holiday

A Mandate From the Board

As information and technology have become major components of an organisation's ability to do business, the role of the Chief Information Officer has evolved to reflect the growing importance of this topic. As IT has converged with business at large, the role of the CIO is now in the centre ground.

> "Security was always looked at like something that was off to the side. What I'm seeing in most companies is that the CIO's role is shifting, and it's becoming more business-facing. That's where we're seeing security re-emerge in its rightful place, right in the middle of it."

Erik Gaston
VP Executive Engagement, Tanium

As securing an organisation's information and technology stack has become a top priority for the board, security budgets have risen. To deliver on this priority, the role of the CISO is also developing. The CISO is increasingly strategically aligned with the CIO and the board to ensure that effective investment in information management and security is delivered.

> "Along with the CIO, the CISO now has a seat at the table with the board of directors and that's been a very positive development."

Zac Warren
Chief Security Advisor, Tanium

However, as CIOs and CISOs seek to gain a clear picture to provide a risk profile to the board, they can be hindered by a lack of clarity and visibility into their IT estate. Many have inherited sprawling IT landscapes with data from legacy infrastructure, on-premises, cloud, and SaaS sources. This can spell trouble for CIOs and CISOs who want to articulate the threat landscape or demonstrate a return on investment clearly.

Converging IT and Security

> "We are trying to move away from the old approach where everything had to go through various security guardrails. You could develop a solution in eight weeks but then spend three to six months waiting for it to gain security approval before it could go live."

Paul Curtis
Chief Technology Officer, Easyjet Holiday

Many of the interviewees we spoke to are turning to SecOps models in an attempt to better manage information risk and increase the visibility and useability of IT assets. SecOps involves a convergence between security and IT operations. By enabling security to have a seat at the table at the earliest inception of a new product or service, businesses can eliminate security blocks later down the line.

> "It's short-sighted to try to design without having the security team involved in that process right at the beginning."

Barry Panayi
Chief Data & Insight Officer, John Lewis

While efforts to introduce or expand SecOps are a positive development, many organisations are held back from fully realising this strategy because they lack a foundational understanding of the tools, processes, and technologies used by each discipline. Without this level of understanding, it becomes challenging to drive efficiency, innovation and effectiveness between IT operations and security teams.

"Retrofitting security afterwards is typically more expensive and typically takes longer."

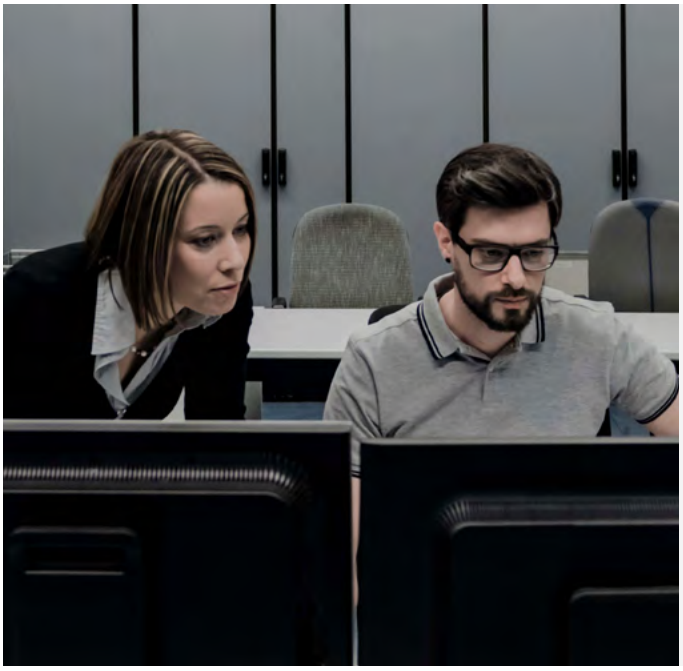
Que Tran
Regional Chief Information Officer, DP World

SECTION 2

Expectations Versus Reality

As organisations move from strategy to implementation, expectation gaps often emerge. Through interviews with senior information and security experts and leaders from across a range of industries, we identified the most common misconceptions leaders had faced while on their journey to converge and innovate IT operations and security. In the next section of this report, we lay out the expectations and the realities as described by our interviewees. We also set out a series of principles senior leaders can apply to deliver better technology risk management.

"Many organisations have lost visibility because they have inherited architectures and environments that were implemented by their predecessors. They made the best decisions they could with the technology, processes and people that they had at the time, but now we realise that there are gaps in the security," says Zac Warren, the Chief Security Advisor, at Tanium.



> **"There's always a gap between aspiration and implementation. That itself is a recognised risk that must be appropriately managed."**
>
> **Chief Information and Security Officer**
> FTSE 100 packaging business

Tool Proliferation Versus Tool Optimisation

The attack surface has exponentially grown through the expansion of the information economy and the development of increasingly sophisticated tech stacks. In these complex environments, security vulnerabilities can appear, reappear and multiply overnight. As firewall and VPN solutions alone have been acknowledged as inadequate to protect modern enterprises, the response for many organisations has been to acquire a wide range of new cybersecurity tools.

"Cybersecurity capabilities are actually very good. The lack of integration of capabilities is where the gap is for many businesses," says Erik Gasto, the VP Executive Engagement, at Tanium.

While this has matured the overall security risk posture, it has also increased the complexity of the complicated IT ecosystem. Counter-intuitively, an increase in tooling to address security threats could be making the problem worse, if those tools fail to integrate together. As such, many organisations had grappled with how to oversee, manage and optimise their existing information and security ecosystems. Many organisations have duplicate functionalities and underutilised applications.

> "I use the tooling that's already available to the best of its ability before I flag the gaps."

Matthew Wilmot
Group Head of Enterprise IT & Information Security, Fraser Group

For organisations in this position, focussing on tool optimisation to get the most out of existing tools could be a more effective strategy. This starts with gaining clear visibility of the assets in use and identifying ways to optimise and integrate those tools. From this vantage point, vulnerabilities can be more effectively identified and more quickly addressed.

> "Figure out how to fully utilise the tools you have. Get rid of all the noise, all the extra software and all the extra things that you're not utilising and then reassess where your gaps are. It's about simplification for me."

Zac Warren
Chief Security Advisor, Tanium

A Single Pane of Glass Versus Multi-Paned Windows

> "Trying to get the single pane of glass is incredibly difficult, but there are ways to create what we class as oracles of truth."

Chief Information and Security Officer
FTSE 100 packaging business

A single pane of glass is a management strategy involving unifying data across several sources and presenting it back as a single view. As businesses become increasingly data-rich and data-dependent, senior leaders need to consolidate the information coming in and out of their organisation from various sources. An expectation emerged that this flow of information can be managed through a single executive dashboard.

Through our interviews, we found that achieving a single pane of glass isn't always effective in consolidating the information needed to answer business critical questions. Many businesses have too much information and too many critical business questions to be answered at pace and this makes a single pane of glass unrealistic.

Instead, leaders are developing multi-paned windows to address multiple key business problems by integrating and combining different tools and collapsing information onto a pane per business problem. By bringing together data from different corners of a business environment, leaders are equipped with a realistic picture and gain a holistic view of the risks associated with business-critical data and applications.

> "Directly correlate what you're doing to resolving business problems. Then, collapse information onto control planes that directly relate to solving those business problems. That's transformative. Transformation should be simple, not complex."

Erik Gaston
VP Executive Engagement, Tanium

Compliance Versus a Risk-Based Approach

> "Focus your budget because no one has a blank chequebook for security and there are limited people with the expertise for it."

Zac Warren
Chief Security Advisor, Tanium

Organisations can protect themselves against numerous risks through compliance.

But the expectation that being compliant equates to being cyber-resilient is largely inaccurate. Compliance and regulation often focus on narrow areas and encourage a tactical, tick-box approach. This can leave security vulnerabilities and gaps unchecked.

> "Of most importance is our commercially sensitive data and our customer data. For the rest, we have a different level of security."

Barry Panayi
Chief Data & Insight Officer, John Lewis

Among the experts we spoke with, many were in the process of bridging the gap between compliance and a risk-based approach that preempts and mitigates risks.

Our interviewees commonly cited the need to make risk assessments in order to focus their resources and expertise on critical data in high-priority business areas.

Once this is in place, data can then be pulled from multiple sources, analysed and protected in accordance with an evaluation of risk. This provides a holistic view and offers the ability to hone in on business-critical data and applications dynamically, as the needs of the business, and the threat landscape evolves. This approach also creates efficiencies and helps to demonstrate the ways in which security measures can drive revenue.

> "We've begun to look much more at graduated controls and rightsizing for operating environments and research environments."

James Tomkins
Chief Architect, Met Office

But to realistically implement a risk-based approach, businesses must know where their business-critical data and applications sit. They must have visibility across their IT ecosystems and organisational processes in place to avoid tool and information sprawl.

Complexity Versus Simplicity

> "Significant efforts have been made to simplify the policy landscape because security has often been seen as too complex."

James Tomkins
Chief Architect, Met Office

Many organisations accept that added complexity is inevitable on the journey from on-premises infrastructure towards public cloud. Yet as digital transformation shows no signs of abating, organisations are recognising that they can not manage unchecked levels of complexity.

Following the pace and scale of digital transformation, businesses are recognising that too much complexity holds them back from innovating and from understanding their vulnerabilities. To combat this, many of our interviewees had embarked on programmes to simplify their IT ecosystems.

As businesses seek to implement risk-based approaches to information and security management, it is becoming clearer that being able to catalogue data, assets and information coherently and to track that through the organisation is a key starting point.

> "If you don't have that basic visibility, then you can't understand your vulnerabilities. And so for me, that's the largest gap most organisations have between expectations and reality."

Zac Warren
Chief Security Advisor, Tanium

"Having observability into the organisation to see what's happening is a priority for us. At a meaningful business level, we want to see what's happening in the business on a day-to-day basis," says James Tomkins, the Chief Architect, at the Met Office

"We're simplifying our overall estate. From a security and data standpoint, it's much easier to manage a single set of resources that can be scaled, instead of lots of disparate systems. That simplification really reduces the complexity and makes it much more difficult for there to be various holes."

Paul Curtis
Chief Technology Officer, Easyjet Holiday

SECTION THREE

Guiding Principles for Better Information Risk Management

As organisations seek to overcome old expectations and implement realistic strategies for effective information risk management, a number of guiding principles can help. In the next section of this report, we summarise the most cited pieces of advice shared by the senior information, data and technology leaders interviewed for this report.

IT Hygiene

> "IT hygiene is really the foundational element. Once you have that in place, you can move more into risk management, culture change and ultimately cyber resilience."

Chief Information and Security Officer
FTSE 100 packaging business

Businesses that want to meaningfully develop their organisation's cyber resilience must resist quick fixes or hype-fuelled solutions. Often, more tooling that promises to be the panacea can add to the problem by creating additional layers of complexity in the ecosystem.

"A core component of security is good hygiene. The elephant in the room when it comes to cyber is the lack of IT hygiene, which means being able to see all your assets and being able to assess your vulnerabilities. It's a huge gap, unfortunately," says Zac Warren, the Chief Security Advisor, at Tanium.

In pursuit of cyber resilience, businesses must double down on IT hygiene. Gaining the clarity needed to make strategic progress requires an accurate view of an organisation's entire IT estate. It's essential to effectively organise cloud, on-premises and SaaS assets before accurate data about the risk can be gleaned.

This involves keeping IT assets tidy and orderly by ensuring that inventories are up-to-date and complete. The importance of these foundational steps can not be overstated. By minimising common concerns pertaining to the health and hygiene of an IT estate, it becomes simpler to determine what risks and vulnerabilities are present.

Automation

> "We are currently looking at how we can make standard inventories more automated."

Barry Panayi
Chief Data & Insight Officer, John Lewis

While implementing and maintaining IT hygiene is essential, it can be a time-consuming business. The manual effort of taking IT, application and data inventories can also be inefficient and subject to human error. Even for the most skilled security experts, gathering data from a plethora of specialist tools with limited interoperability hinders their ability to gather timely and context-rich information.

"We want our developers to work in a completely unconstrained way, knowing that everything they do goes through automated quality processes and procedures. We use the build process to call out anything that's not passed our security standards."

Paul Curtis
Chief Technology Officer, Easyjet Holiday

By automating processes relating to IT hygiene and security maintenance, a business can free up their talent to focus on projects that are strategically aligned with business goals. This helps to turn security-related activity from a cost centre into a revenue generator.

"An integral part of being able to do this successfully is looking at the mechanisms we can use for automation. Because relying on large manual efforts doesn't deliver business value. So we'll have to build a lot of this with automation to provide that observability. Otherwise, it becomes very difficult because things move so quickly," says James Tomkins, the Chief Architect, at the Met Office

> **"Just expanding our security teams isn't a long term solution. Right now, we can't identify threats quickly enough or defend at the speed of light. Automation, integration and interoperability is our means to demonstrably realise and meet the businesses long term security objectives."**

Chief Information and Security Officer
Government department

When an endpoint might be in jeopardy, automation also enables incident teams to speed up response times by providing a fast and accurate picture of the environment in minutes instead of days.

> **"Automating what we do day-to-day helps to solidify and protect an organisation."**

Ketan Patel
Group Chief Information Officer, WH Smith

Collaboration

Along with improving processes and technology, a key component of better information risk management is culture. Central to success is the ability to move security from a silo to an integral part of the business.

This begins at the top of the organisation, with more collaborative working between CIOs, CISOs and the board. It expands into ways of working, by ensuring that security professionals are part of the design and delivery not only of the overall IT agenda but the overall business agenda.

> "SecOps models are important because it shows a different kind of mindset into how security fits into the overall operations of the organisation."

Que Tran
Regional Chief Information Officer, DP World

The introduction of SecOps models seeks to achieve this aim, by encouraging greater collaboration between security teams and IT operations. In order for SecOps models to successfully move from strategy to implementation, businesses must gain a deep understanding of the tools that have traditionally underpinned each discipline and find ways to meaningfully integrate them to enable siloed teams to come together in impactful ways.

> "It's short-sighted to try and innovate without having the security team involved right at the beginning."

Barry Panayi
Chief Data & Insight Officer, John Lewis

By driving greater collaboration between security and IT operations teams, organisations can increase the visibility of both security risks and IT priorities to dually drive business growth and resilience. By integrating and automating across security and IT operations, further benefits can be achieved in the form of agility and efficiency.

> "Collaboration with your team and the collaboration with your leadership really pays off. By collaborating through the journey, delivery is a lot more timely and cost-effective."

Senior Manager
CERT, Vodafone

> "Security was deemed as a topic that employees couldn't engage with easily and so switched off from. As a result, it fell into the hands of a few specialists. To counter this, we introduced wide-spread communication and education programmes across the organisation to embed security as everyone's responsibility."

James Tomkins
Chief Architect, Met Office

CONCLUSION

The Whole is Greater than the Sum of its Parts

> "Many businesses are trying to solve complex cybersecurity threats with linear solutions. But the risk landscape doesn't present itself as a series of linear problems. For a dynamic problem like security, businesses will need to look more at integrated platforms that provide the complete picture."

Erik Gaston
VP Executive Engagement, Tanium

As information and security management evolves and matures further, professionals in this area will continue to have their expectations defied. But by leaning on guiding principles, organisations can introduce risk-based approaches and collaborative models that make security an integral part of doing business, thus closing the gap between expectations and realities.

Dynamic, ever-changing problems like security need a solution that is greater than the sum of its parts. No one solution, team or methodology will provide a quick fix, because to solve dynamic problems you need integrated solutions. To achieve a strategic and pre-emptive approach, businesses must focus on optimising and integrating the tools they have and consolidating them to provide a better birds-eye view of the threat landscape.

> "Gaining visibility does more than it says on the tin. It not only massively reduces risk, which is a huge factor, but it also accelerates innovation because we can see what data assets we have within the organisation."

Jon Roughley
Director of Data Strategy and Innovation, Experian

CHIEF DISRUPTOR

Chief Disruptor is the community for business and technology leaders.

Disruptive leaders believe like us, that disruption is a catalyst for the opportunity and our name, Chief Disruptor, proudly embodies and celebrates that mindset. Since 2005, our membership community for business and tech leaders has brought together innovators, change-makers, and disruptive thinkers to share expertise, strategies and actionable insights.

Our purpose has always been to cut through the hype and enable our members to leverage these disruptive trends and technologies through our member-led insight reports, content, and community activities.

With ongoing geo-political unrest and the grim reality of recession on the horizon, organisations now more than ever, need nimble, purposeful leadership that grasps the opportunities and proactively manages the threats of disruption. It's not going to be easy, but we are here to help guide you. Connect. Learn. Disrupt. chiefdisruptor.com

TANIUM

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments.

Only Tanium unifies teams and workflows and protects every endpoint from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. Tanium has been named to the Forbes Cloud 100 list for seven consecutive years and ranks on Fortune's list of the Best Large Workplaces in Technology. In fact, more than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.