The new era of digital trust

Expanding beyond cybersecurity towards societal digital future readiness

A discussion with Mark Brown, Global Managing Director, Digital Trust Consulting Services, BSI

bsi.

Contents

Abstract

Author: Mark Brown

Global Managing Director, Digital Trust Consulting Services, BSI

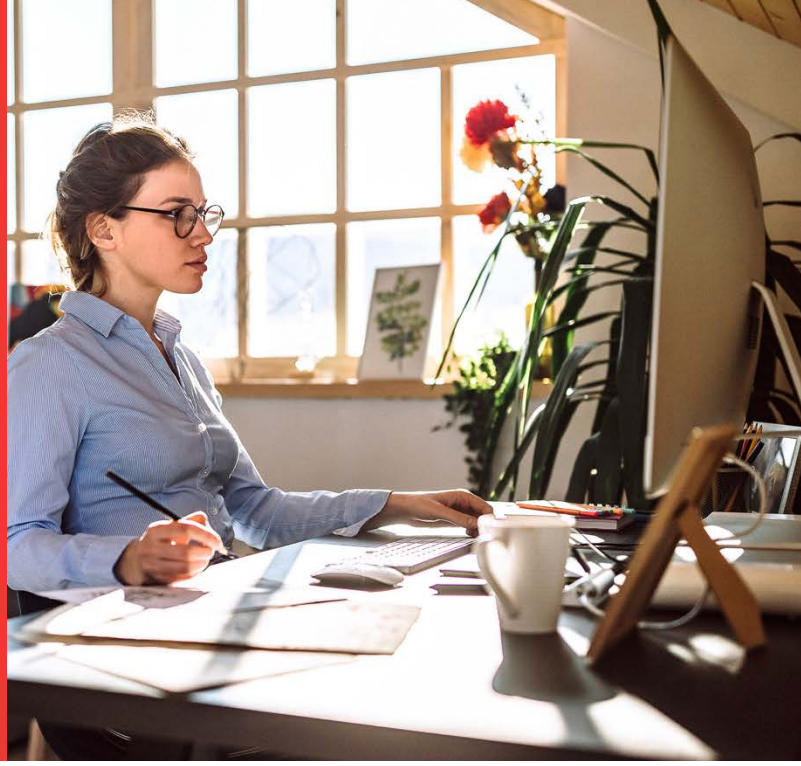
Brown has over 30 years' experience in cybersecurity, data privacy and business resilience consultancy. He has previously held roles at Wipro Ltd. and Ernst & Young, among others. His wealth of knowledge includes extensive proficiency on the internet of things (IoT) and the expanding cybersecurity marketplace, at all times focusing both on the strategic enablement and risk protection elements of cybersecurity.

In our increasingly connected world, newfound risks including misinformation, digital deception and a blurring of the lines between personal and digital safety are now threatening organizational and societal trust in digital systems and technologies.

In this paper, Mark Brown discusses:

- organizational and societal implications of accelerated digital transformation;
- how society is now moving away from the traditional challenges of technology and cyber risk, to a more widespread business and operational risk
- the challenges of mapping and managing the risk of distributed digital supply chains
- how building and instilling digital trust is key to ensuring the success and resilience of those operating in the digital sphere moving forward

"Today, both businesses and society as a whole need to become more agile and adaptable when operating within the ever-changing landscape of information technology."



A shift in the status quo

Over the last two decades, an increasing reliance on digital systems has drastically altered how societies around the world behave and function. This trend has been accentuated by the COVID-19 pandemic, during which many industries have undergone accelerated digital transformations, employees have shifted to remote or hybrid working models, and platforms, systems and devices facilitating this change have multiplied. Whilst the migration of society to this new digital world shows no signs of relenting, the threat of cybercrime looms larger than ever, consistently costing businesses around the world tens, or even hundreds, of millions of dollars.

Cybersecurity threats are growing in frequency and sophistication, with malware attacks tripling, and ransomware attacks quadrupling in recent years. The negative implications are not limited to organizational impacts such as financial loss and brand reputation. Such incidents can also cause damage to transport infrastructure, information and communication systems, social cohesion and individual mental health can be put in jeopardy.

These major cyber-attacks are now outpacing organizations and societies' ability to effectively prevent or respond to them, in truth organizations are having to sprint to stand still in the face of this tsunami of cybercrime.

This has instigated a monumental shift in the status quo. In the past, organizations generally adopted a cybersecurity and risk management program focused heavily on managing threats and protecting their business environments (an often laborious approach that can slow business operations and inhibit innovation and adaptability).

Today, however, both businesses and society as a whole need to become more agile and adaptable when operating within the ever-changing landscape of information technology. It is essential that cybersecurity programs effectively no longer focus on trying to intercept every attack on your environment but rather evolve their detection and response capabilities to enable and support critical business functions, while simultaneously guaranteeing the continuity of operations. In short, this means developing an approach that balances the impact of a cyber-attack with the ability to maintain normal business operations.

"In the new digital society, when technology fails, operations is the area that's hit hardest. When operations fail, financial revenue impacts are almost instantaneous."

Making the move from a technology focused discussion to an operational discussion

To broaden that conversation from simply focusing on the implications of technology, to looking at the situation from a broader business and operational angle – the key is to educate the organization (the user) as to why it's necessary.

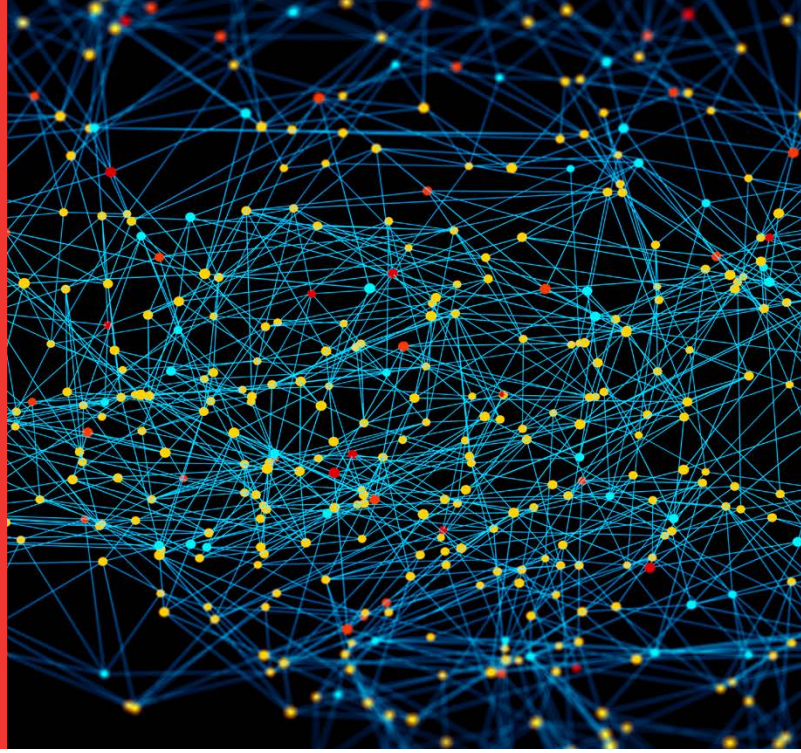
Many organizations talk about the importance of the Chief Digital Officer or the Chief Data Officer, yet these things have been systemic in our businesses for many years. We don't talk with organizations about having a 'Chief Electricity Officer' because electricity is systemic to society, and everybody has it.

At BSI, we forecast that within probably five years, nobody will be talking about the Chief Digital Officer or the Chief Data Officer because it will just be systemic and normal for organizations to have those roles.

The key is to remove the mystique from technology, to make it consumable and understandable to all levels of an organization. The role of a CIO or a CISO will still be very important in the future, but what we're seeing evolve as the mainstay and one of the main decision-makers is the role of the chief operations officer.

In the new digital society, when technology fails, operations is the area that's hit hardest. When operations fail, financial revenue impacts are almost instantaneous and they can be in the tens of millions of dollars per hour for a major company. So, translation to the common language, the lingua franca of business being about business risk and business operations, is the key step change that we are seeing organizations make.

"There is no such thing as an information security process. There is no such thing as an IT process. There is a business process, which is enabled by IT and protected by information security."



Advice for CxOs

For the last two or three decades, organizations have largely seen IT and cybersecurity as cost centers to a business rather than a strategic asset, resulting in a culture that does not value technology and the highly skilled technologists that manage it.

Because of that view of IT, leadership often thinks it can be outsourced to save money and provide the same benefits as an internal IT department closely aligned with leadership. However, when that happens it creates a disconnect between the business and IT, as technologists are simply viewed as workers that deliver technical solutions to the business without truly having to understand how those solutions can help the business.

On the flipside, IT operates in a world of processes that don't necessarily mean anything to business executives and board members. In the real world, there is no such as thing as an IT process or a cybersecurity process. There is only a business process that requires IT or cybersecurity enablement.

For example, new employees need access to their organization's data, and when they are elevated to high positions or leave the company, their level of access needs to reflect those changes. However, that doesn't happen without IT.

Having been a Fortune 10 global CISO myself, I came to understand the role of the Chief Operations Officer very well. I came to understand how the business operated. I came to understand the actual core business of how the business runs.

My guidance to the CISO would be: If you only ingrain yourself in technology, if you only align yourself to the CIO, are you going to be able to facilitate that translation to the wider business?

The key is to gain an understanding of what your business actually does. What's the core reason for its existence? I've always said and maintained: "There is no such thing as an information security process. There is no such thing as an IT process. There is a business process, which is enabled and protected by information security."

That, for me, is the key role of the CISO. Understand the business processes you're supporting, understand what could go wrong if that business process fails, and then discuss with the CEO and the business leadership, at the business level, the role and support that can be provided – and really focus in on the business impact.

Digital supply chain risk

Within the open cloud environment that we see today, plus the acceleration of digital transformation, risk relating to digital supply chains has been substantially exasperated. About 20 years ago, it was very easy for an organization to understand their landscape of operations. They could put a big firewall around their environment and point to the perimeter.

However, we are in now a new era of de-perimeterization. Every organization has both a physical and a digital supply chain, but the problem with the digital supply chain is that unlike your internal IT environments, where you can decide what controls are in place and what security is positioned in the environment, within the digital supply chain, you're relying upon the third party making the right choices.

BSI has about 77,500 clients in 195 countries, and they tell us that the digital supply chain is one of their core cybersecurity risks. In a recent survey of over 150 clients, 73% of organizations said that it was number one on the CISO agenda and the COO agenda. Not one organization we spoke to felt it was in control of that area.

With BSI being at the forefront of development in best practice in cybersecurity, this was a key indicator to us that we really needed to grasp that space, to help companies understand what the risks were and how to manage them, and to develop solutions to help those organizations and wider society understand and address the impacts of digital supply chain risk.

"By mapping out your solutions, by understanding which vendors are outside your environment and where they sit within the value chains and within the business process, you start to map out where the critical risks are."

Mapping out the process

Gaps around the digital supply chain can be very difficult to identify. It's not simply who you have a contract with.

There is third-party, fourth-party and fifth-party risk.

There is upstream risk, midstream risk and downstream risk.

Understanding the connectivity points goes back to mapping out the business process.

When many organizations look at the technology landscape, they only look at what technology solutions they have. They don't map it to the business process.

By mapping out your solutions, by understanding which vendors are outside your environment and where they sit within the value chains and within the business process, you start to map out where the critical risks are.

It's not just the size of the contract – that's a common mistake many organizations make. Just because you spend millions with one organization doesn't make them a critical risk.

A good example would be the company you use to do your annual report. The three to four weeks before that gets published, that's some of the most sensitive data in your company, especially if you're stock market listed. Yet, that can often be one of the smallest contracts a company has annually and one that's not often considered from a cybersecurity perspective.

So, really understanding the sensitivity of the data and the criticality of the business process, and then mapping out the vendors into that business process and value chain is a key step.

"Digital trust is all about not just protecting an organization from the negative aspects of business and technology risk but about how the organization can strategically enable its company and accelerate its company through digital transformation."

Addressing the new era of digital trust

Digital Trust is not the new name for cybersecurity. Instead, it encompasses a much larger pool of factors that influence customer, user and stakeholder trust in an enterprise. Our vision is to support clients in the digital era, ensuring interactions between business, people and things are engaging, secure, trusted through evidence and profitable enterprise.

To address this new era of digital trust, BSI Group has expanded its consulting practice beyond just cybersecurity to take on broader questions around digital trust, helping customers address everything from digital supply chain risk to the ethics of artificial intelligence.

BSI has been at the leading edge of many developments in the world of information and cybersecurity for over 30 years. In 1995, BSI authored the forerunner to what is today ISO 27001. We've seen within BSI that clients are spending significant amounts of money on technology and digital transformation, and they're doing it for a number of reasons.

Post-COVID, the need for digital has accelerated and we're seeing a new digital economic society form. And while all the old aspects of cybersecurity continue to be required to protect the impacts of negative risk, we're also seeing clients ask,

- How do I know I'm making the right investments?
- How do I know I'm getting value for my money?
- How do I know that what the vendors are telling me I'm spending money on is actually going to deliver the benefits?

So, digital trust is all about not just protecting an organization from the negative aspects of business and technology risk but about how the organization can strategically enable its company and accelerate its company through digital transformation.

We help them leverage four key areas –

- cybersecurity and privacy
- digital governance and risk management
- digital supply chain
- data stewardship in the ethics and governance of AI

By taking both the positive enablement and the protective aspects of technology risk. Our clients are finding those are very useful services, which allow them to translate a very technology-based discussion into a new business discussion, which is understood by the wider organization.

“Digital trust is about instilling confidence in an organization, that empowers the people, the systems and the technology to ensure their safety, security, compliance, privacy and ethical requirements”

Mark Brown, Global Managing Director, BSI Digital Trust

About BSI

At BSI, we have a long and proud heritage dating back to 1901. In 1929, we were awarded our Royal Charter which sets out what we do, and why we do it, allowing us to be transparent about our purpose. In 1995, we developed the world’s first information security standard.

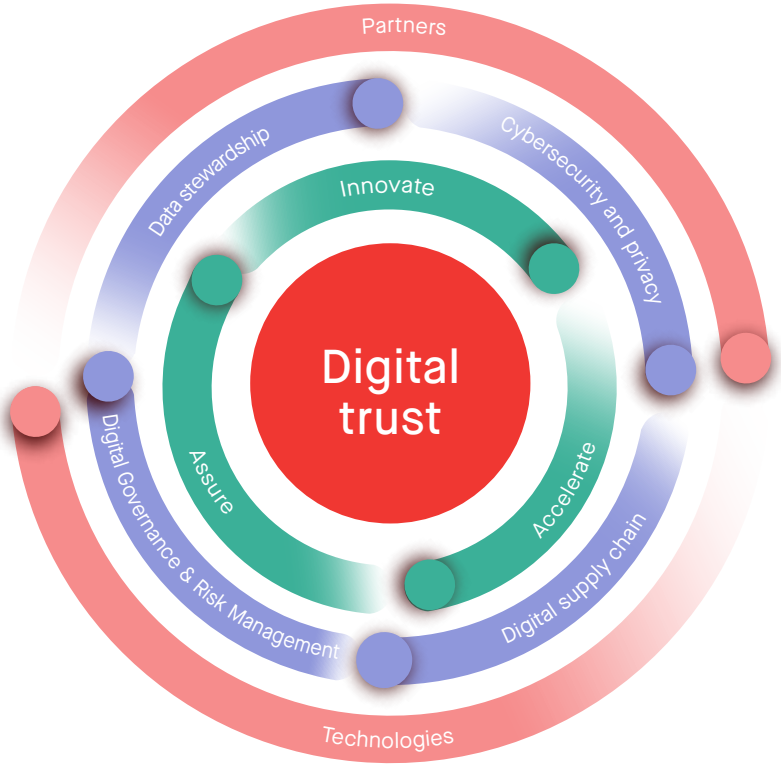
Today, we partner with over 77,500 clients across 195 countries to establish digital trust with their employees, customers, shareholders, and communities by protecting their cybersecurity and data privacy. We are committed to inspiring trust for a resilient world in everything that we do, every day.

About BSI Digital trust

At BSI Digital trust, our global expertise enables our clients to better enhance their cyber resilience, protecting their critical information and IT infrastructure, people, and brand reputation. We support organizations through our integrated portfolio of services including providing digital and cyber risk advisory, security testing services to clients, as well as looking at areas like data privacy, compliance and governance, as well as niche capabilities such as e-discovery and e-forensics.

Digital trust aggregates four subdomains with interlocking strategies, plans, and actions:

1. Cybersecurity and privacy
2. IT Governance and risk appetite
3. Data stewardship and AI ethics
4. Digital supply chain



Get in touch

EMEA
Call: +353 1 210 1711
Email: digitaltrust.consulting.IE@bsigroup.com
Visit: bsigroup.com/digital-trust

UK
+44 345 222 1711
digitaltrust.consulting@bsigroup.com
bsigroup.com/digital-trust

US
+1 800 862 4977
digitaltrust.consulting.US@bsigroup.com
bsigroup.com/digital-trust

Subscribe to our newsletter

Follow us on