



accelerate your ambition

Cybersecurity for the digital age



If you believe you can do anything,
we're here to help you do it.





A story about **collaboration, innovation, and possibility**

Welcome to our primer on the future of cybersecurity as an enabler of innovation. I promise it isn't just another dry trend report about security in the digital world – there's a very good chance you won't fall asleep while reading it – and you'll get to explore some real-world examples of near-future technologies that could directly impact how you integrate security into your digital world.

This exploration began with the Dimension Data Security team's annual conference, where we came together to exchange ideas, understand trends, and update our strategy for the coming year. From this meeting it was patently obvious that the security industry is moving incredibly fast and we need to move with it. It was critical that we not only understand the here and now in the security industry, but where it could go in two years, five years, and even further into the future.

Soon after the conference, I was introduced to MJ Petroni and the Causeit team's innovative work in other areas of NTT; the timing couldn't have been better. Dimension Data decided to partner with Causeit to put together a futurist book, and I think the story behind it is an important one about collaboration and innovation.

After months of dialogue and research – and the comedy of trying to schedule meetings for a distributed team in two organisations and four continents – this book is the result of us working together to explore the future of cybersecurity from a new perspective. The ideas and case studies here reflect what I believe is driving innovation within the security industry, and some of the changes I expect to see in the very near future.

Digitisation is driving many of the changes we're seeing in security, and we have to move from device sales to outcome management to partner with our clients on the journey of digital transformation. The security paradigm has to be reviewed, renewed, and re-enacted to shift away from fear-based to opportunity-based, allowing cybersecurity to provide new value as an enablement tool for businesses and consumers alike.

We're acknowledging that while everyone needs security, no one likes to live in fear. If we accept the requirement that business and consumers need to evolve, then we as security professionals and as an industry, need to do so as well. For me personally, the most exciting thing about this paradigm shift is that cybersecurity truly does become an enabler of business, of lifestyle, of healthcare, and of a better society. And as a leader in the industry, I feel really good about that.

Enjoy the read,

Matthew Gyde
Group Executive, Security

Contents

Page **04**
The evolution of data, digital systems, and control

Page **07**
Changing how we think about security

Page **12**
A closer look at IT's evolution: today, tomorrow, and the future

Page **29**
What's on your horizon?: The technologist's challenge

The evolution of **data,** **digital systems,** and **control**

The first enterprise computers were so expensive that much like executive salaries, any one organisation could only afford a few, and they had to be centralised. As the cost of computing decreased, using a remote terminal to run programmes on a central server started to make less sense, and companies began using desktop machines. Modems and the early consumer networks of CompuServe, Prodigy, and AOL segued into the age of the Internet and the World Wide Web, making it possible for information to

flow much more freely than ever before. But the way data flowed – relying on user commands and poorly configured networks – made it an unreliable way to exchange important information.

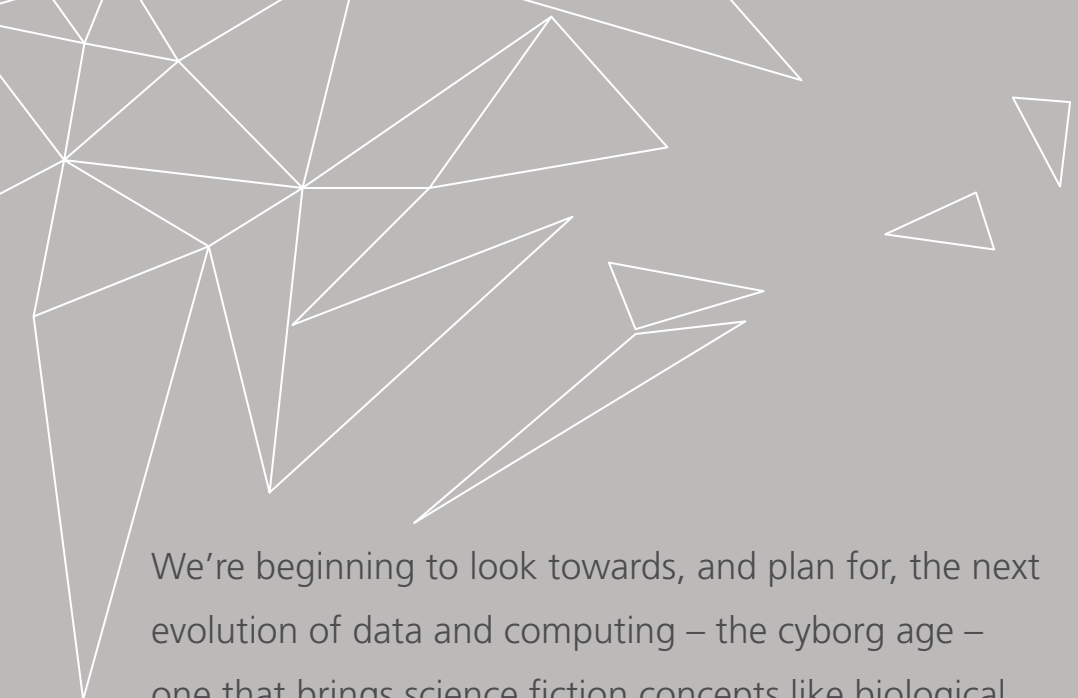
As the Web evolved, social networks and cloud-based products challenged the effectiveness of using desktop Operating System (OS) email and attachments to send and receive information. In the IT world, the emergence of cloud computing represented a synthesis of the old models of centralised computing and the new models of innovation and independence, fostered by an empowered workforce and connected customers. But the data we'd structured, and the security, stability, and speed of the networks it travelled on had a lot of catching up to do. As clouds become the norm, the way we conceive of innovation and risk is changing. Almost any application or device can be connected to the Internet, and vast pools and streams of data have become key assets for both individuals and companies.

At this point, creating a fixed technology infrastructure or strategy just doesn't make sense. Applications and infrastructures are now being built with an agile mindset, able to be adapted quickly to purposes not originally conceived of by their coders. The cloud promises huge potential for collaboration, and exponential increases in value, speed, and efficiency, but brings with it an explosion of potential risks and vulnerabilities.

‘Driverless cars and biological, digital implants are just the beginning’

**To talk to us about how to accelerate
your digital business with hybrid cloud**

[➤ Click here](#)



‘creating a fixed technology infrastructure or strategy just doesn’t make sense’

We’re beginning to look towards, and plan for, the next evolution of data and computing – the cyborg age – one that brings science fiction concepts like biological augmentation and artificial intelligence into focus. Cyborgs, short for cybernetic organisms, are a way of thinking about a near future where the distinction between our human selves and our digital selves becomes less clear. We’re already moving into this age. For example, think of how much more capable we’ve become by using a smartphone with mapping and translation tools during international travel rather than paper maps and street signs. We’re even experimenting with previously unthinkable concepts like implanting chips into our bodies and augmenting our senses of sight, touch, and hearing with digital input.

Driverless cars and biological, digital implants are just the beginning of an era when digital technology could become crucial for our survival and quality of life. As a culture, we’re largely unprepared for the legal, regulatory, and social implications of this evolution. Technologically, there are still many complex problems we must solve to make technologies of convenience reliable and safe enough to become technologies of survival. If we’re going to move into the future responsibly, and manage the risks that come with these new opportunities well, we’re going to have to shift our ways of thinking about data, privacy, the nature of business, and security.



Changing how we think about security

In the next two to five years, entirely new ways of storing, sharing, and using data will require a major shift in how enterprises think about identity, value, and security.

A blurred, high-angle photograph of people walking on a paved sidewalk, overlaid with a green geometric pattern. The text is contained within a white-bordered box in the upper left.

Organisations are **shifting their cybersecurity strategy from reactive to agile.**

Organisations are no longer merely reacting to threats. Instead, they are creating IT infrastructures—and even entire enterprises—which are agile and adaptive, where breaches are addressed before they happen.

To talk to us about how to accelerate your digital business with cybersecurity

➤ [Click here](#)

A solid green background with a white geometric pattern of overlapping triangles. The text is contained within a white-bordered box in the upper right.

Cybersecurity is **changing its focus from devices to services.**

While tools such as firewalls have become standard for securing devices and zones, risk management in the digital age requires a big picture, managed-service approach which can protect entire IT ecosystems over time.



Organisations are evolving **from discrete entities into networks.**

Digital value creation requires shared data, and that means networked individuals and networked organisations. Risk management can't simply shut off less secure systems, it must adapt to include them without compromising core data security.

Data is moving **beyond silos and into pools and streams.**

Data is no longer strictly assigned to specific departments, applications, or even individuals, but is being shared across and between organisations.

A closer look at IT's evolution:

today, tomorrow, and into the future



Here and now

Today's enterprises are beginning to see the opportunities of the future come into focus, but many are still trying to keep their legacy systems stable and secure.



Just ahead

In the next two to five years, entirely new ways of storing, sharing, and using data will require a major shift in how enterprises think about identity, value, and security.



On the horizon

Over the next 10 years, and beyond, enterprises will evolve rapidly, taking full advantage of opportunities for digital innovation, and working together to secure the clouds of data that have become essential for business and daily life.



Here and now

Today's cybersecurity and technology landscape is complex. The hulking mainframes of older legacy technologies are in sharp contrast to the clouds above them – and it's difficult to decide which systems to modernise first. Hybrid IT blends old and new models of risk management to make new value possible, without abandoning old investments.



Here and now

During this first phase of digital data evolution, when data must move from one company to another, it goes from an application, through the OS to a storage device, out through networks to another company's device, through its OS and into a new application. The points of vulnerability are somewhat limited to a few key network ports. Perimeter-based security requires engineers to create firewalls around the organisation. Generalist CTOs build architectures based on the bigger picture of how the network

is secured against outside threats, while allowing information to flow to and from trusted partners. Then, IT managers control and allow access to certain zones of the network. Most organisations using this mode of cybersecurity rely on these limited internal roles to design and manage their cybersecurity strategy, and a few work with managed service providers to accomplish these goals, but such perimeter-based cybersecurity won't be sufficient to carry organisations into the future.

‘perimeter-based cybersecurity won’t be sufficient to carry organisations into the future’



Here and now

Data sharing is essential to the creation of new digital business products such as Web apps and mobile apps, which integrate customer information through an application programme interface (API). However, opening company data up is risky too, so IT leaders must balance the risk and reward of new digital business value with the cost of creating properly-secured systems.

Currently, companies vary widely in their tolerance of innovative, peer-to-peer technologies and collaboration tools, resulting in a challenge to attract and retain ‘millennial’ workers, and innovate at the pace of digital-first companies disrupting traditional business.



Here and now

Innovation debt is a critical element of this equation. Deferred innovations create a ‘debt’ when the time to access those investments comes along and they aren’t there to support new offerings or reactions to competitors. Meanwhile, ‘legacy debts’ around older technologies arise as a talent issue. For example, many companies

have modern Web interfaces that are linked to older mainframes for certain functions and newer, cloud-based systems for others. In the event of a breach or the deployment of a new application, engineers must be able to maintain functionality of these hybrid systems with a broad skill set that is difficult to source.



Here and now

PayPal is an early example of innovation in Security-as-a-Service (SECaaS). It acts as an intermediary solution for weak, perimeter-based systems where sensitive data can't be secured. Over time, e-commerce customers have shown they feel safe using PayPal to make purchases online, even if the appearance and credentials of a vendor site aren't good enough for them to feel comfortable directly entering credit card information.

By offering this layer of credibility as a service, and addressing fraud problems that are too complex for smaller vendors to manage, PayPal and other platforms like it, enable online business to thrive without the costly or restrictive need to secure individual transactions or records.

'Most companies will have to share both customer and operational data with other organisations'

To talk to us about how to accelerate your digital business with digital infrastructure

[▶ Click here](#)



Here and now

In the near future, innovation will require that risk management shifts its focus from the perimeter of the organisation to the increasingly vital links between organisations for data exchange. Most companies will have to share both customer and operational data with other organisations as part of larger, platform-based digital offerings. For example, an insurance provider may share data with healthcare providers for better claims management, with customer apps for improved experience, or with academic institutions for research.

Data diplomacy (selective, consensual, and intentional sharing of data for mutual benefit) will become a critical skill for most organisations in the next five years. The effectiveness of organisations' big data policies and tools will become evident in the quality of their digital offerings, and the security around them, and forward-thinking organisations will earn first-to-market or first-to-scale advantage by being able to securely and effectively monetise their access to data.



Just ahead

It'll soon be commonplace for data to move laterally from one company's applications and servers to another and back, 100s or 1000s of times per user action, across a diverse set of network and application environments. In this environment, perimeter-based cybersecurity isn't effective, so the data itself must be secured as it moves. Cybersecurity at the user level is evolving towards this as well, with a shift to tokens, authentication, and single sign-on (SSO).

'Computer Emergency Response Teams (CERTs) and engineers with full-stack expertise will be increasingly important'



Just ahead

As threats become more frequent, more sophisticated, and more dangerous, organisations begin to struggle with managing cybersecurity on their own. The needs are too complex to be managed by the general IT department, and there simply aren't enough information security professionals to go around.

As a result, managed security roles such as Computer Emergency Response Teams (CERTs) and engineers with full-stack expertise will be increasingly important to provide for this gap in internal capability.

To talk to us about how to accelerate your digital business with cybersecurity

[Click here](#)



Just ahead

To manage risk and security in the near future, companies must focus on balancing the need for rapid innovation with the cost of modernising and securing legacy IT systems. Increasing cloud adoption will require that all organisations manage endpoint security. Some new applications need the data itself to be secured so that it's safe from attack

while moving between systems, or so thoroughly anonymised that user information is protected. However, organisations who do well at securing data will be able to take on daring innovations their competitors can't risk, or protect themselves from public relations disasters that their less-secure competitors will inevitably face when customer data is breached.

'organisations who do well at securing data will be able to take on daring innovations their competitors can't risk'

To talk to us about how to accelerate your digital business with workspaces for tomorrow

[▶ Click here](#)



Just ahead

With HomeKit and HealthKit, Apple has brought its platform model of value sharing into very private realms: users' homes and health. As an early example of the Internet of Thing's (IoT) potential, these platforms share and combine data for the user's convenience and personal benefit. However, they also represent an opportunity to share your data – either with organisations for research

purposes, or with Apple to inform what options the platform offers you in the future. This opportunity creates a new, combined cybersecurity need at the user level as well as in the organisations that are receiving/using the data, which will become commonplace in the near future.

'agile organisations who have mastered the security of their systems will have a competitive advantage'



On the horizon

Ten or more years in the future, agile organisations who have mastered the security of their systems will have a competitive advantage, and will be able to selectively unlock and extrapolate data for enormous societal and individual benefit.

The edges of the organisation will become increasingly less relevant as significant strategic partnerships form between digitised companies. It's likely, however, that organisations who take the lead in exploring new digital business models and offerings

– autonomous vehicle companies, for example – will become targets for increasingly skilled cybercriminals. These organisations will need new, agile strategies for managing and designing secure IT to manage the risks that come with accelerated innovation and evolution.

To talk to us about how to accelerate your digital business with cybersecurity

➤ [Click here](#)



On the horizon

Significantly secured platforms and APIs will continue to play a major role in securing the exchange of data to enable innovative new business models. Technology decisions will be made from a full-stack mindset, not just around specific components, and data will be in near constant motion as it passes through the many systems analysing it. Other emerging technologies, which could be more widely adopted for security and identity management include: cyborg or machine fingerprints, gestural and behavioural signatures, and biometrics. Much as social networks require one-time granting of access between

parties ('friending' someone) and then let information flow freely between those trusted parties, machine-centric security ('trusted devices') and transparent authentication of users will allow for effective security with less friction than we experience now.

'Technology decisions will be made from a full-stack mindset, not just around specific components'



On the horizon

In a world where machines can make decisions together – and grant access to one another – information security will require experts to keep those machines healthy and safe. We'll also need detectives and researchers who can investigate threats, which may not even involve a human perpetrator, and architects who can design flexible cybersecurity strategies to handle the variety of human and machine actors in the network, without restricting the flow of data which makes everything work.

‘With a robust security infrastructure, driverless cars promise breakthroughs in automotive safety, speed, and ecological sustainability’



On the horizon

Digitised transport: driverless cars

Advanced application of digital models in the analogue world means that unprecedented opportunities are possible, and with them comes new types of risk. With a robust security infrastructure, driverless cars promise breakthroughs in automotive safety, speed, and ecological sustainability. As we venture further into an age of mass orchestration of semi-

automated or fully autonomous cars, vulnerabilities could expose not only the contents of a parked car that can be remotely unlocked, but core systems like braking, acceleration, and steering. Already, most major automakers have discovered digital security issues in their connected cars, which needed to be patched quickly and remotely.



On the horizon

IoT: connected home

Platforms coming to market today such as Nest and Apple’s HomeKit offer to connect individual devices such as utility meters and appliances to each other, to the cloud, and to a single-user interface. These platforms enable opportunities for home-sharing, lower security costs, and the potential for savings through the highly coordinated management of energy and other resources.

Having your car tell your air conditioner to turn on shortly before you arrive home from work, or gamifying energy use across a neighbourhood by sharing metrics from connected appliances, could bring enormous value to consumers and conservation efforts. However, a home which can be unlocked and relocked remotely via the cloud, with dozens (or hundreds) of virtual access points connecting the home network and any sensitive data it contains to the cloud, will present an entirely new cybersecurity issue for homeowners.

‘platforms enable opportunities for home-sharing, lower security costs’

What’s on our horizon?

Cybersecurity makes it possible to take smart risks in the service of exploring great opportunities.

If cybersecurity is too restrictive or generalised it can stifle the creation of new digital value. Today’s IT leaders are trying to choose between prioritising innovation to protect market position and the need to lockdown systems and mitigate risk.

With the tools available in most enterprises, these may seem to be the only options. Modern security infrastructures, however, can allow for massive innovations and security at the same time. With the right timing and investments, world-changing innovation is possible.

Accelerate your digital business



**digital
infrastructure**



hybrid cloud



**workspaces
for tomorrow**



cybersecurity

➤ **Start your journey to greatness**



About the author and contributors **MJ Petroni & Jessica Long**

As California-based Cyborg Anthropologists working closely with the NTT Group, the world's largest telecom, Jessica and MJ focus on the changes our world will experience in the next hundred years through the lens of the relationship between humans and technology. As key business leaders visit NTT's Innovation Institute, the team has in-depth conversations with them about the possibilities—and ethics—of technologies such as artificial intelligence, the Internet of Things (and its coming successor, the Social Network of Things), big and little data, nanotechnology and robotics in domains such as financial services, government, healthcare, education, and automobility.

MJ is the owner and founder of Causeit, Inc. (www.causeit.org)—part futurist think tank and part innovation consultancy. He also serves as a founding advisor

to the Bill and Melinda Gates Foundation's Global Digital Financial Services Platform for poverty alleviation. MJ and Jessica have presented on many global stages, for example, RSA (the world's largest cybersecurity conference) and SIBOS (SWIFT's global financial event). His team also co-produced TEDxBellevue and are currently authoring the living book, *Cybiomes: Biology, Technology and Hope*.

Matthew Gyde

Group Executive, Security Solutions

Neil Campbell

Group General Manager, Security Solutions

Kenneth Mead

Digital Storyteller

Natasha Horwitz

Senior Marketing Manager

Middle East & Africa
 Algeria • Angola
 Botswana • Congo • Burundi
 Democratic Republic of the Congo
 Gabon • Ghana • Kenya
 Malawi • Mauritius • Morocco
 Mozambique • Namibia • Nigeria
 Oman • Rwanda • Saudi Arabia
 South Africa
 Tanzania • Uganda
 United Arab Emirates • Zambia

Asia
 China • Hong Kong
 India • Indonesia • Japan
 Korea • Malaysia
 New Zealand • Philippines
 Singapore • Taiwan
 Thailand • Vietnam

Australia
 Australian Capital Territory
 New South Wales • Queensland
 South Australia • Victoria
 Western Australia

Europe
 Austria • Belgium
 Czech Republic • France
 Germany • Hungary
 Ireland • Italy
 Luxembourg • Netherlands
 Poland • Portugal
 Slovakia • Spain • Switzerland
 United Kingdom

Americas
 Brazil • Canada • Chile
 Mexico • United States