Let's talk,
Secure transformation
by **design**

YULCOM
Technologies

HITACHI
Inspire the Next
Hitachi Systems Security Inc.

DFFRNT

About us

We are your strategic Digital Trust partner for global cyber risk management and mitigation since 1999!

HITACHI SYSTEMS SECURITY INC. AT A GLANCE

24/7 Managed Security Services/Products

Professional Security and Privacy Services

CERTIFICATIONS

- ISO 9001 certified for managed security services
- ISO 27001 certified for managed security services
- SOC II Type 2 certification
- Member of the Forum of Incident Response and Security Teams (FIRST)
- PCI Qualified Security Assessor (QSA)
- SWIFT Cyber Security Services Provider (CSSP)
- Recognized employee expertise (CISA/M, CISSP, PCI QSA/ASV, ISO 27001 LA, GCIA/H, CEH, CRISC, CGEIT, CIPP/M, etc)

Canada
Switzerland
Japan
India

● SECURITY OPERATIONS CENTERS

TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030

1 Supply chain compromise of software dependencies

2 Advanced disinformation campaigns

3 Rise of digital surveillance authoritarianism/ loss of privacy

4 Human error and exploited legacy systems within cyber-physical ecosystems

5 Targeted attacks enhanced by smart device data

6 Lack of analysis and control of space-based infrastructure and objects

7 Rise of advanced hybrid threats

8 Skill shortage

9 Cross border ICT service providers as a single point of failure

10 Artificial Intelligence Abuse

THREATS 2030

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Ransomware continues to be an ongoing issue for companies globally.

The True Cost to Business, EDR vendor Cybereason notes 73% of companies studied[1] indicated they had been targeted with at least one ransomware attack in the preceding 24 months.*
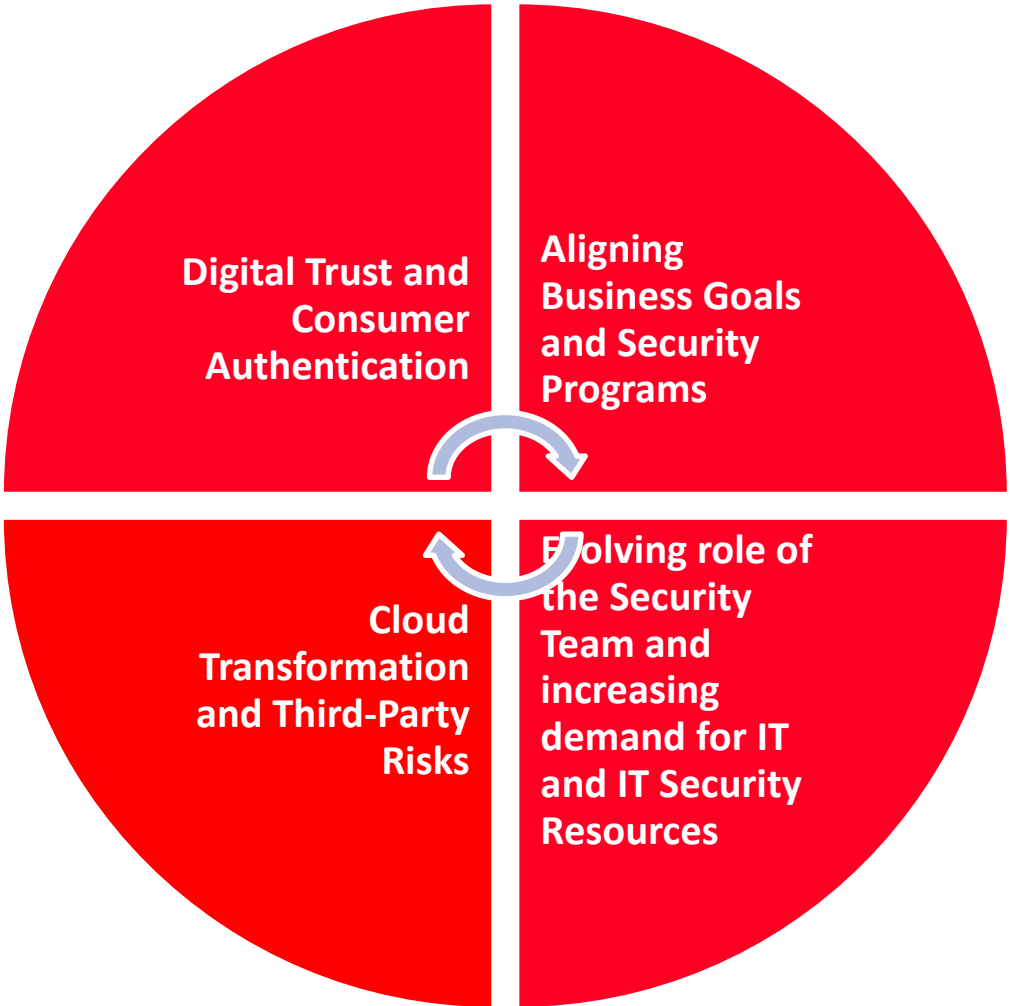
Adoption of and Adaption to DX needs Real-time Cybersecurity Measures

With DX , companies are increasing their surfaces for attacks vis-à-vis complex and increasing volumes of attacks. Therefore, a disciplined approach to cybersecurity resilience and maturity is required at all levels.
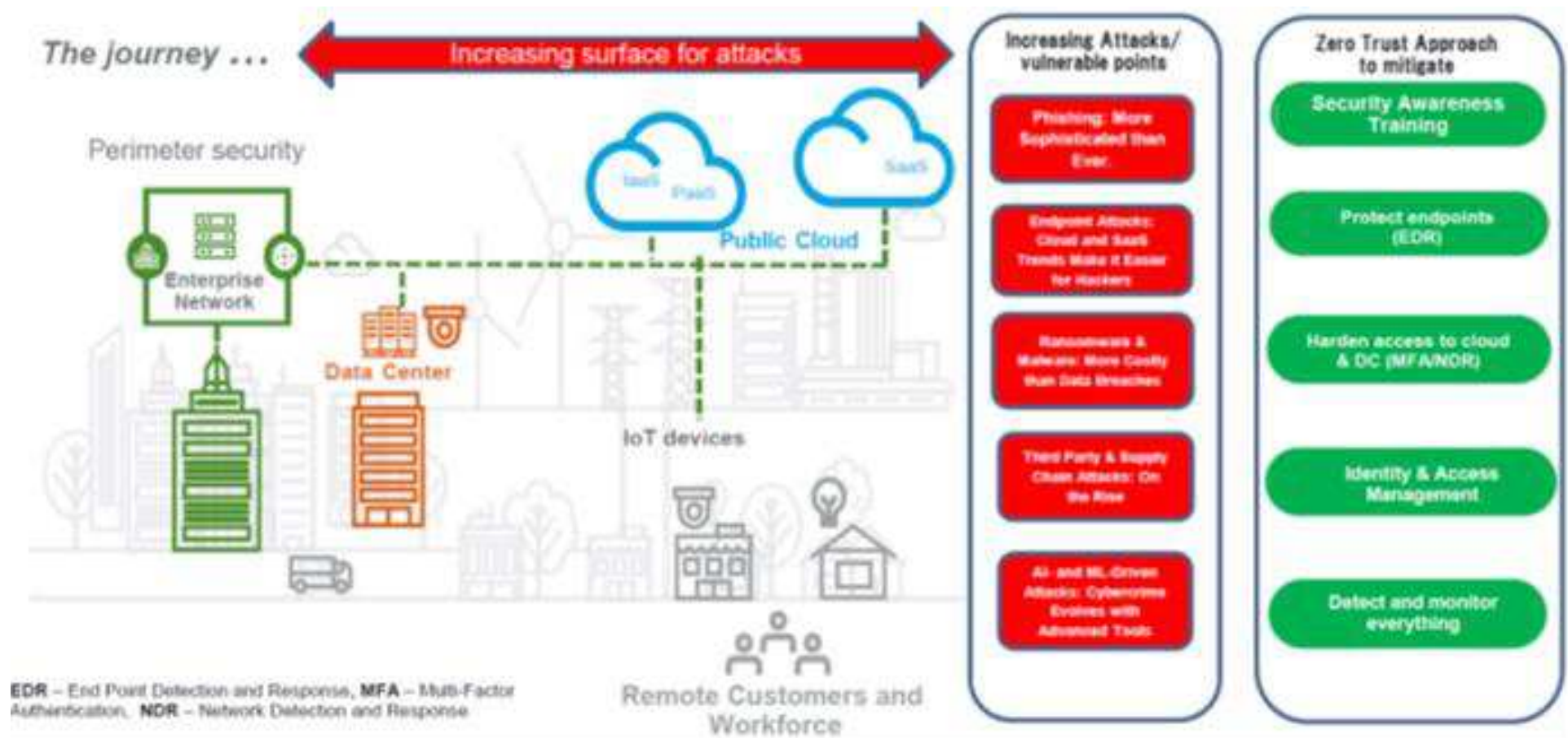
Secure Transformation by Design is not just about Technology…

➢ It is a **data-centric game**. Digital Trust is crucial Secure Transformation by Design.

➢ Understand the **data intelligence requirements** – who owns the data you are retrieving, where is it coming from, and how is it going to be leveraged?

➢ As companies progress on their transformation journey, they must think holistically and adopt a risk-based approach to determine where investments are required for security. The business goals must along with the security programs.

Digital Trust and Consumer Authentication

Aligning Business Goals and Security Programs

Cloud Transformation and Third-Party Risks

Evolving role of the Security Team and increasing demand for IT and IT Security Resources

➢ As an organization moves deeper into the cloud journey, security/privacy by design must be embedded throughout each step.

➢ Ensure there are relevant controls early into the product/service life cycle, and evaluate the security maturity of the critical providers in the supply/value chain.

➢ As companies put more investment into technology, the Information Security Team must make a valuable contribution. Security cannot be an afterthought. It's worth noting that digital transformation is driving the demand globally for IT and Information Security resources.
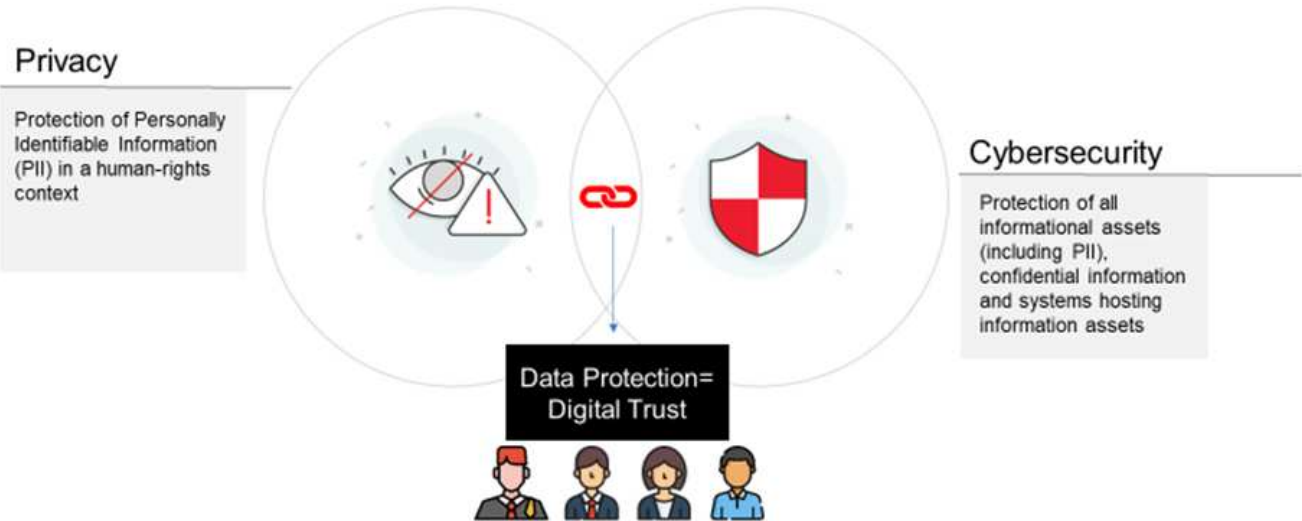
Trust is the Imperative, but it is not left only to IT…

Digital trust must be a key objective in a company's digital transformation journey.
It requires a balanced investment in Digital Transformation and Data Protection, that will require support from all stakeholders, starting with the Board of Directors.

Several Layers of **Digital Transformation**

- Infrastructure
- Customer Experience
- Culture
- Business Model
- Organization
- Processes
- Leadership & Capabilities

Privacy and Security **by Design**

Privacy
Protection of Personally Identifiable Information (PII) in a human-rights context

Cybersecurity
Protection of all informational assets (including PII), confidential information and systems hosting information assets

Data Protection= Digital Trust

Invest in People, Processes and Technology

Key Takeaways

1. ALIGN BUSINESS GOALS AND SECURITY IMPERATIVES

To manage costs and ensure that business and security priorities are aligned, organizations should leverage automation where possible, and enhance their cyber functionality by incorporating AI enabled cybersecurity solutions with human expertise.

2. BUILD DIGITAL TRUST AND CONSUMER AUTHENTICATION

Due to the pandemic, there is a shift from traditional services to on-line services. This trend has grown exponentially post-pandemic. **The organization that masters the digital customer experience is likely to enjoy the greatest market share.** Ultimately, customers will likely go wherever the interactions are easiest and where they feel safe and secure.

3. ADAPT TO OR MAINTAIN REGULATORY REQUIREMENTS

Increasingly, particular attention is placed on organizational resilience in which the protection of data is a fundamental component. Many countries are enacting data privacy laws to comply with key elements of the General Data Protection Regulation (**GDPR**) or their own privacy laws. Within these laws, **data security forms a key principle that includes data encryption, effective monitoring, and incident response and reporting for data breaches.**

4. ADDRESS THIRD PARTY DUE DILIGENCE AND UNGOVERNED CLOUD ADOPTION

Not all organizations are prepared to quickly pivot operations through Digital Technology given their infrastructure and limited internal resources. This ed to the services of solutions providers and **the rapid adoption of cloud technologies, that may not have undergone the required level of security design and assessment rigor**. In the initial stages, this could expose these organizations to unknown vulnerabilities and 3rd party risks.

5. DEVELOP, EMPOWER, AND FOSTER BETTER COLLABORATION WITH THE ORGANIZATION'S SECURITY TEAM

While the cybersecurity team remains a collection of technical and operational compliance professionals, we are seeing a transformation of a more business strategic, forward-looking responsibility. Many Chief Executive Officers (CEOs) work closely with their CISOs as a trusted and relevant voice at the strategy table and in satisfying digital trust and regulatory requirements in a manner that is efficient from a time and cost perspective.

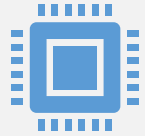Digital Transformation
Montréal 05.2023

www.yulcom.ca

About Us

- YULCOM Technologies is a Canadian software engineering firm specializing in custom digital platform and website development as well as IT project management, applying big data and AI.

- YULCOM has positioned itself in the digital transformation market and offers its services to a growing number of clients (Desjardins, Government of Canada, Enabel, University of Montreal, Bell Media, Organization International de la Francophonie, World Bank, UNDP, etc.).

- Whether it's software, web applications, CRM or websites, our company is committed to offering custom solutions to its customers and relying on Open Source technologies and most reliable frameworks.

YULCOM
Technologies

What is a digital transformation?

Use digital technologies to make significant changes to an organization's operations, business models, and strategies

Digital transformation encompasses a wide range of technologies and initiatives, including cloud computing, artificial intelligence (AI), big data analytics, the Internet of Things (IoT), automation

Successful digital transformation can lead to numerous benefits, such as increased operational efficiency, enhanced customer satisfaction, improved agility, and the ability to capitalize on new business opportunities

However, it's important to note that digital transformation is an ongoing journey, as technologies and customer expectations continue to evolve.

Why do we need a digital transformation?

The goals of digital transformation may vary depending on the organization, but we can expect:
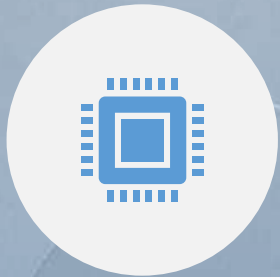
Improving customer experience: Digital transformation enables organizations to better understand customer needs, personalize interactions, and provide seamless and convenient experiences across multiple channels.
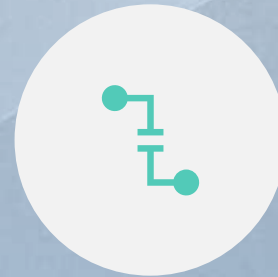
Enabling data-driven decision-making: With access to vast amounts of data, organizations can leverage advanced analytics and AI technologies to gain valuable insights, make informed decisions, and identify new business opportunities.

Enhancing operational efficiency and improve productivity.

Empowering employees: with tools and platforms that enhance collaboration, communication, and knowledge sharing, leading to increased productivity and job satisfaction.

Facilitating innovation: Digital transformation encourages organizations to explore new business models, products, and services that leverage emerging technologies to stay competitive in a rapidly evolving digital landscape.

![YULCOM Technologies logo]

1500 College Street, Suite 400
Montreal, QC H4L 5G6

www.yulcom.ca

514 375 6190

info@yulcom.ca
ejuanpablo@yulcom.ca

Who we are

DFFRNT leverages deep understanding of human behavior, leading technology and new business models to design valued, **"dffrnt"**iated experiences.

From strategic insights and analysis of customer and user behaviour, combined with inspired creative design, we architect the user experience to meet organizational goals.

Dominira Saul, M.Sc.
FOUNDER & PRINCIPAL

20 years in user experience, human factors, user research, interaction design

- P/T Faculty, University of Ottawa, Digital Transform & Innovation
- You.iTV Director UX
- Partner & Chief Experience , Akendi
- Principal, usabilityagency.com
- MSc User Interface Design
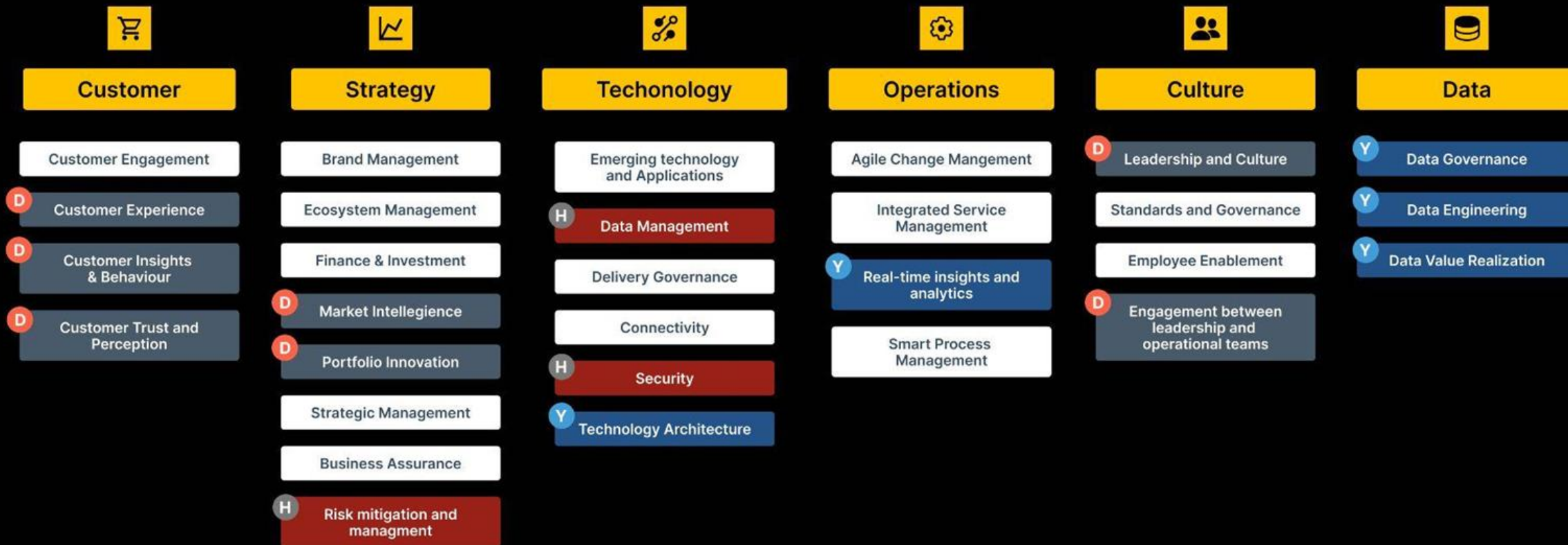
Shaun Illingworth, Ph.D.
FOUNDER & PRINCIPAL

20+ years experience in product and service design research, human factors & design innovation

- P/T Faculty, University of Ottawa, Digital Transform & Innovation
- Shopify Senior Experience Lead
- Managing Director & Partner, Akendi
- Nortel Innovation lab
- PhD, Exp. Psych, Boston

Typical Stages of Digital Transformation

Customer	Strategy	Techonology	Operations	Culture	Data
Customer Engagement	Brand Management	Emerging technology and Applications	Agile Change Mangement	(D) Leadership and Culture	(Y) Data Governance
(D) Customer Experience	Ecosystem Management	(H) Data Management	Integrated Service Management	Standards and Governance	(Y) Data Engineering
(D) Customer Insights & Behaviour	Finance & Investment	Delivery Governance	(Y) Real-time insights and analytics	Employee Enablement	(Y) Data Value Realization
(D) Customer Trust and Perception	(D) Market Intellegience	Connectivity	Smart Process Management	(D) Engagement between leadership and operational teams	
	(D) Portfolio Innovation	(H) Security			
	Strategic Management	(Y) Technology Architecture			
	Business Assurance				
	(H) Risk mitigation and managment				

From a human-centered design point of view, the stages of digital transformation typically involve the following:

1. Research and Discovery:

This stage involves understanding the needs, behaviors, and pain points of the users or customers. It includes conducting user research, interviews, surveys, and other methods to gather insights about their preferences, expectations, and challenges.

2. Ideation and Conceptualization:

In this stage, the focus is on generating ideas and concepts that address the identified user needs and align with the organization's goals. Design thinking methodologies, brainstorming sessions, and collaborative workshops are often employed to encourage creativity and innovation.

3. Prototyping and Testing:

Once concepts are generated, the next step is to create prototypes or mockups of digital solutions. These prototypes can be in the form of wireframes, interactive mockups, or even functional prototypes. User testing and feedback collection are crucial during this stage to evaluate the usability, desirability, and effectiveness of the proposed solutions.

From a human-centered design point of view, the stages of digital transformation typically involve the following:

4. Iteration and Refinement:
Based on the insights gained from user testing, the digital solutions are refined and iterated upon. Feedback is incorporated, and the design is adjusted to improve the user experience, address pain points, and ensure that the solution aligns with user needs and organizational objectives.

5. Implementation and Deployment:
Once the digital solution has been refined, it moves into the implementation and deployment phase. This involves the development and coding of the solution, integration with existing systems or infrastructure, and ensuring the solution meets security and privacy requirements.

6. Evaluation and Continuous Improvement:
After deployment, it's important to evaluate the effectiveness of the digital solution in meeting user needs and achieving business objectives. User feedback, analytics, and metrics are used to assess the solution's performance and identify areas for further improvement. This stage involves a continuous feedback loop to ensure ongoing refinement and optimization of the digital solution.

It's worth noting that these stages are not strictly linear and may overlap or be revisited as part of an iterative design process. The focus on human-centered design ensures that user needs and experiences remain at the forefront throughout the digital transformation journey.

Getting the balance right is essential, and difficult to do without a deep understanding of users, their goals, behaviours and psychographics.

Too little security

Too much security

- Lack of trust from end users
- High risk for enterprise

- Difficult to use
- Low user retention
- Users are prone to try and circumvent security measures
- Leading to high risk for enterprise (that thinks they're well protected)

Getting the balance right is essential, and difficult to do without a deep understanding of users, their goals, behaviours and psychographics.

Economic landscape – There are a lot of compelling reasons that business are pivoting towards self-serve.

- Operational Efficiency
- Market Pressure
- Customer Convenience

However in order for self-serve to be successful (whether internal or external to the organization) there needs to be trust in the security without overwhelming users.

In order to be successful, enterprises need to:

- Build security and trust into overall digital transformation
- Understand dark patterns in trust (AI, voice interaction, conversational AI) (voice infantilizing of).
- Support end users in their goals and tasks.
- Find "trust triggers" that matter to their user/customer base.

1- How do we create a risk mitigation program to avoid ..

2- How can human-centric design in digital transformation help organizations mitigate the risk of cyberattacks and enhance overall security posture?

3- What are the key steps organizations should take to address human error as a major factor in cybersecurity breaches, and how can user experience be leveraged to promote secure and optimized operations?

4- In light of the evolving threat landscape, what strategies and best practices can organizations implement to ensure that digital transformation initiatives are deployed with proper risk management and governance, minimizing potential disruptions and security risks?

Let's talk,
Secure transformation
by **design**