HITACHI

Inspire the Next

Hitachi Systems Security Inc.

DIGITAL TRANSFORMATION

Digital Transformation in the Financial Industry

DIGITAL TRANSFORMATION FOR CUSTOMERS

With the changing landscape, clients want solutions that are agile, scalable, customizable and cost effective to meet the increasing needs of the customers. Digitalization has become essential to enable fast and secure online services and products , but cyber attackers are focusing on these systems.

What does this mean for the financial sector?

Digital trust becomes the key component of loyalty. Trust still is a key pillar for any Financial Institution.

Organizations need to invest in People, Processes and Technology

1 ALIGNING BUSINESS GOALS WITH SECURITY IMPERATIVES

To manage costs and ensure that business and security priorities are aligned, financial institutions automate and enhance their cyber functionality by putting more AI enabled cybersecurity solutions.

RECOMMENDATION

Think holistically and adopt a risk-based approach on where you need to invest.

1.Implement the proper Governance Structure with a defined Data Protection pillar.

2. Consider what risk scenarios and the controls required relevant to your business and strategies and all customer/employee touchpoints.

3. Embarking on digital transformation requires an almost real time security technology. Automating (**AI EDR/NDR solutions**) your cyber and risk management processes could be seen as a silver bullet in improving your cyber security posture.

DIGITAL TRUST AND CONSUMER AUTHENTICATION

2

Due to the pandemic, there is a reduction of in-branch services and an increase of on-line services. We believe this trend will continue, as there is now a consumer behavioral change. **The Bank 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.

RECOMMENDATIONS

It is a data centric game, so it is crucial to understand data intelligence requirements.

1.Make it a priority to understand the privacy and data concerns around how, and by whom, your data is going to be used. Much of it will most likely be in the cloud, so think about how to encrypt and protect it.

2. Be alert on the movement of data and related services/processes. Recognize that these processes span both internally, and externally through 3rd party providers. Be cognizant of 3rd party risks, since you are only as secure as the 3rd party in your supply chain.

HITACHI
Inspire the Next
Hitachi Systems Security Inc.

Regulators now require some form of enforcement by institutions to adopt a 'data-centric' 'security and 'privacy-by-design' approach, as the global cyber threat landscape continues to increase.

THE NEXT WAVE OF REGULATION

3

Since the start of the pandemic, particular attention has been 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 reporting for data breaches.**

RECOMMENDATION

Demands from a variety of regulators are increasing.

1.Appoint an individual to oversee data privacy regulatory compliance, e.g., **Data Protection Officer**. This individual must work closely with the Information Security and Legal Teams.

2.It is critical to institute ongoing testing of your regulatory compliance program in terms of design, implementation and effectiveness to identify where improvements are needed and to ensure operational cyber resilience is embedded into your overall architecture and processes.

CLOUD TRANSFORMATION AND THIRD-PARTY RISKS

4

Some financial institutions were largely not prepared to quickly pivot their operations through Digital Technology given their current infrastructure and limited internal resources.

This required 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 'go-live' stages, this exposed these banks to unknown vulnerabilities and 3rd party risks.

RECOMMENDATIONS

Accelerated adoption of third-party solutions introduced new risks never seen before

1.As you move into the cloud journey, **security by design** must be enabled through each step.

2.Ensure there are relevant controls adopted early into your product life cycle to deliver maximum value to both customers and users.

3.Have a clear understanding of the entire data flow, ensuring enterprise connection between business enablement, business resilience, and information protection in your cloud transformation strategy.

4.Conduct 3rd party due diligence for all critical suppliers that includes information security maturity validation, and the right to audit.

5.Evaluate the 3rd Party Risks within your ERM and Risk Appetite acceptance level.

HITACHI
Inspire the Next
Hitachi Systems Security Inc.

While new technology is seen as an opportunity, it comes with new vulnerabilities, threats and governance challenges.

THE EVOLVING SECURITY TEAM

5

While the Cyber security 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.

RECOMMENDATION

One of the biggest challenges for security professionals is translating knowledge into an actionable appreciation for what it actually means to the business.

1.Given the increasing complexity of technology and cyber threats, the evolution of the information security accountability needs to shift away from the IT department, and into a specialized unit with qualified Information Security Experts, e.g. Operational Risk Department. This unit must be empowered with the support from the C-Suite/Board.

2.As you invest more into technology, the information security team must make a critical contribution in the required conversations from a strategic perspective, planning, design, and implementation. Information Security cannot be an afterthought.

3.With the exponential adoption of digital transformation, the demand for IT Security resources (as well as IT Resources) will increase significantly. Banks need to adopt the relevant hiring, training and retention strategies to navigate through this. Outsourcing or supplementing with a security service provider is another option, e.g. CISOaaS or InfoSecaaS.

Consumer Confidence vs Increasing Cyberattacks

74% of Financial Institutions have reported an increase in cyberattacks during the pandemic.

56% of consumers want greater transparency from their financial institutions about the impact of cyber crime

55% of consumers actively consider cyber crime protection when choosing financial institutions

53% want more guidance from financial institutions on how to behave online

Data Protection Pillars towards Digital Trust

HITACHI
Inspire the Next
Hitachi Systems Security Inc.

Governance	Architecture Design	Prioritization of critical data assets	Application in Production	Business Resilience	Security Awareness
Must be part of your ERM Framework Security Security Program relevant to your business strategy	E2E Security by Design or Privacy by Design adoption **People** **Processes** **Technology**	Prioritization of Critical Data and Assets **Zero Trust** Identity Access Management policy and practice	**24/7 monitoring** and Security Privacy Controls Review	Failover capability Data backup and Restoration	Training for staff and customers to **build the competencies** and to drive behaviour

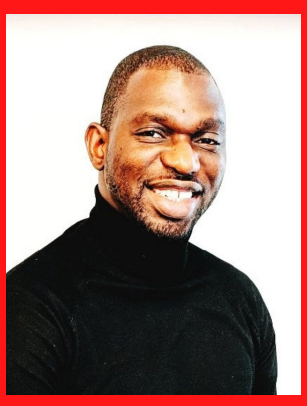
...It's not only about technology, the right Culture is critical

Improving Cybersecurity and Privacy Maturity is a culture shift, at targeted levels.

It is not only the Tone at the Top. It requires ownership at each level.

BOARD OF DIRECTORS	EXECUTIVE MANAGEMENT	LINE MANAGEMENT
Be aware of Cyber threats & Privacy issues	Align resources to risk	Understand threat vectors
Ensure an effective security program	Measure success of cyberdefence and privacy	Delivers intelligence from internal and external sources
Understand risk exposures & determine alignment to Risk Appetite	Ensure return on cybersecurity investment	Integrate cyber-intelligence and Privacy into operations

We are here to help you



David Green,
VP of Sales
david.green@hitachi-systems-security.com

Marisol Litalien,
North America
marisol.litalien@hitachi-systems-security.com

Stephen Juteram,
Caribbean
stephen.juteram@hitachi-systems-security.com

Patrik Heuri,
Europe
patrik.heuri@hitachi-systems-security.com

Hitachi Systems Security World Headquarters
955 Michèle-Bohec Boulevard, Suite 244
Blainville, QC J7C 5J6
Canada

www.hitachi-systems-security.com

T: +1 866-430-8166 (toll free in North America)
T: +1 450-430-8166