Executive Summary

Business Management and Cybersecurity

The perception of cybersecurity as a management task is gradually expanding. However, it is still firmly perceived as a necessary cost. As being cyber-secure becomes the fountainhead of competitiveness amidst soaring business digitization, I suggest repositioning cybersecurity as a competitive edge linked to value creation instead of viewing it as a necessary cost.

--Shinichi Yokohama, NTT Corporation

Business Management and Cybersecurity

The digitization of valued-added corporate assets such as intellectual property and brands elevate digitization of corporate risk. Maintaining cybersecurity means management of digitized corporate risk, and is inseparable from business strategy. The success or failure of cybersecurity management will differentiate business competitiveness within the digital economy.

Cybersecurity is a Business Management Issue

Today the focus is overwhelmingly on data breaches, but those are not the only management risks. Cybersecurity is a management issue primarily because:

- Business continuity may be threatened
- Cybersecurity protects stakeholder trust
- Underpinning digital innovation spurs corporate growth.

Imperative Actions for Business Executives

There are three imperative actions which business executives should take:

1. Prioritize objectives for protection and create layered defense accordingly
2. Ensure early detection, response and recovery as 100% safeguarding is impossible
3. Review all preparations periodically at board and executive management meetings.

Collaboration with Other Companies

Companies can mitigate their workforce and resource deficiencies through mutual collaboration in information sharing and workforce development. As intra-industry firms have similar concerns, and greatly shared needs in terms of workforce and information, collaborating within an industry represents a practical first step. Sector-based Information Sharing and Analysis Centers (ISACs) have arisen within industries.

Global Management

Dealing with cybersecurity from a global standpoint is necessary not only for multinational companies, but for industry as a whole. Global security governance of one's own company is essential. Moreover, it is important to strengthen the supply chain and contribute to international policy harmonization.

Collaboration with Government

Industry should not passively await government policy; rather, it must engage in proactive outreach and advocacy to ensure that its needs are met by government. Action is beginning in the capacity building sphere and should be augmented by information sharing and other means. Cybersecurity is a public good. It is essential that industry plays a proactive role in its establishment and maintenance.

Learn More

Read the complete white paper, *Business Management and Cybersecurtiy* - Digital Resiliency for Executives.
Visit: nttsecurity.com/resources

About the Author

Shinichi Yokohama

Head, Cyber Security Integration

NTT Corporation

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.