Critical Infrastructure Protection and the Cloud

Ken Katayama
Microsoft Japan
Fourth industrial revolution
All powered by the cloud
A Cloud for Global Good

Trusted • Responsible • Inclusive
Aligning Security Baselines For Effective Critical Infrastructure Protection
Some governments are introducing security baselines to manage risk.

Typically defines a set of basic security requirements that aim to minimize cybersecurity risk.

Spans a wide range of operation and risk management activities:

- Protect
- Detect
- Respond
These baselines differ across markets

Americas
- Canada
- Chile
- Colombia
- Mexico

EMEA
- EU and its member states
- France
- Germany
- Kenya
- UAE

Asia Pacific
- Australia
- China
- Japan
- Singapore
PEAK SCENARIO
Convergence on global cybersecurity standards accelerates innovation to promote economic growth and mitigate demographic challenges.

CANYON SCENARIO
If governments take fragmented approaches, innovation and economic development will falter while demographic challenges limit progress.

Aligned security baselines benefit the country.
Companies must take an enterprise-level approach to managing cyber risk

Regulations might impact companies both upstream and downstream.

As the level of risks will differ across different companies and business functions, companies need to take ownership of their risk management approach to create a meaningful impact on security at the appropriate compliance costs.

The nature of critical infrastructure has such wide-ranging implications that companies need to take an enterprise-level approach to manage cybersecurity risks rather than an outsourcing of risks to external ICT suppliers or internal IT operations staff.
Divergent approaches to security baselines would impact critical infrastructure service providers

However, divergent approaches to security baselines across countries create a heavy burden for enterprises operating in critical infrastructure sectors, especially multinationals, by:

• Heightening compliance costs
• Impeding effectiveness of cyber risk management
• Discouraging active senior management participation
• Slowing innovation

When governments that are introducing security baselines align these to international best practices, industry benefits.
Established best practices in managing cybersecurity risks show that both the approach and substance is important.

The six aspects for an effective risk management practice are:

1. Utilize an open collaborative and iterative development process
2. Bridge risk management understanding both within and between organizations
3. Focus on a risk-based and prioritized set of baseline practices
4. Drive toward desired security outcomes rather than prescriptive requirements while recognizing the potential need for more prescriptive and complementary implementation guidance
5. Leverage best practices
6. Realize economic and security benefits with efficiency

Rather than outsourcing risks, each company must take an enterprise-level approach to manage risk holistically.
The NIST Cybersecurity Framework can fulfill these aspects both in its approach and its substance

Approach

The NIST Framework was developed through numerous open workshops on particular aspects of the framework, drawing from diverse expertise and best practices

Substance

• The NIST Framework serves as a single reference point, but is structured according to Functions, Categories, Subcategories and Informative References suited for various audiences
• The NIST Framework provides International Standards ("Information References") without specifying particular controls
• The NIST Framework has maturity models ("Profiles") that enables continuous improvement as enterprises and technology evolve

The U.S. Department of Commerce’s National Institute of Standards and Technology (NIST) developed a voluntary risk-based Cybersecurity Framework for the nation’s critical infrastructure in February 2014, outlining a set of industry standards and best practices to help organizations identify, assess, and manage cybersecurity risks.