RICOH
imagine. change.

A digital security mindset for today's leaders

Ricoh's multi-layered security approach to enabling business transformation and growth

A digital security mindset for today's leaders

Ricoh's multi-layered security approach to enabling business transformation and growth

Overview

Change is inevitable and leaders must continually adapt, especially when it comes to security. As organizations navigate a fragmented landscape of tools and technologies that often reveal security, privacy, and operational gaps, leaders must consider a new approach to business transformation. Reshaping how we incorporate the many facets of security starts at the top and must permeate throughout the organization.

The point: Security has the power to make or break high-level business initiatives, and yet too often it's not addressed strategically.

When we take a top-level holistic view of an organization, security must be seen as a business enabler that drives success in every department and is no longer solely the responsibility of IT — it has evolved into a shared responsibility of executive leadership, involving various internal and external stakeholders.

As organizations transform their operations to achieve business goals, the associated risks increase. Security measures have become a foundational, core requirement that affects compliance, business continuity, brand reputation, business growth, and sustainability.

Early adopters that have embraced a comprehensive layered security methodology will have a competitive advantage, while other organizations may need a tailored strategy.

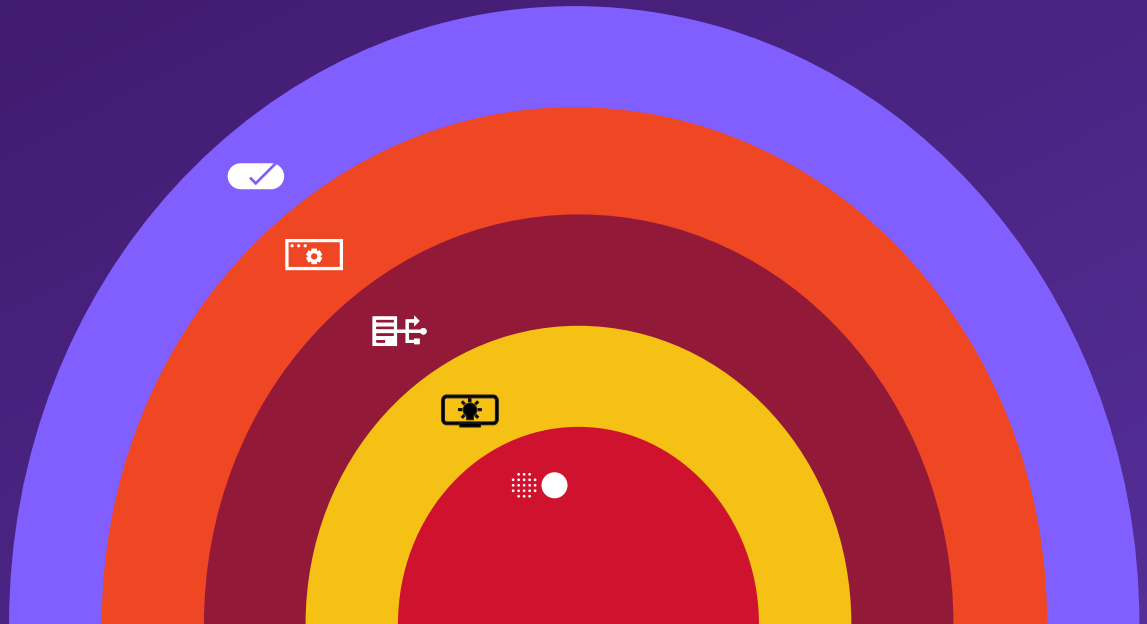
This guide looks at how organizations can make information security strategic to business transformation and facilitate growth with Ricoh using a multi-layered approach.

A new era of security

Increased information security risk and demands from regulators and stakeholders necessitate a strategic security approach that is difficult to orchestrate across the organization. The challenges often result from unstructured data silos paired with the continuous rise in cyber attack sophistication. For businesses of all sizes, we take a systematic and holistic view to help our customers implement a comprehensive security strategy as it applies to information, network, device, application and data security for all types of workforces — remote, hybrid and office.

Ricoh has developed a five-layer approach to addressing and fortifying security throughout any organization to protect company information. If we actively address how security plays a role in meeting compliance, business continuity, brand reputation and growth objectives, we can determine the best path forward within each layer. Let's explore Ricoh's multi-layered security approach.

- **Workforce security**
- **Information security**
- **Device security**
- **Network security**
- **Application security**



Layer 1 – Workforce security

It's easy to make mistakes. Employees can be our best assets but also unintentionally put the organization at risk. Maintaining a high degree of vigilance and adhering to security best practices involves more than just technology — it requires a culture shift that empowers and incentivizes people. With the growing number and quality of cyber threats it can be nearly impossible for organizations to provide sufficient training on their own.

Enable your employees to make smart security decisions every day by delivering a seamless work experience, intelligent tools and secured processes that empower them to be their best. This deters the use of risky 'shadow IT' to work around process issues and makes it easier for them to comply with established policies and procedures.

Solution considerations to enable a secured workforce

- Cybersecurity awareness training
- Information governance consulting
- Documentation
- Support services
- ESG strategy development
- IT Services

Cybersecurity awareness training extends your organization's security to the front lines, making employees aware of the potential risks and educating them on best practices to follow. When coupled with applications, you can train, reinforce, prompt, track and even test your workforce's knowledge to build a culture of praise and vigilance.

Finally, security, information governance and IT strategy consultations can help build confidence with an overarching approach to helping everyone in the organization practice secured ways of working. Our multi-layered approach, based on governance, risk, and compliance best practices, enables leaders to assess risk impact, identify and address vulnerabilities before they impact your business. Not only is a data-driven, secured workforce the right way to promote growth, but it is also a way to deliver a seamless, innovative experience built on trust.

Layer 2 – Information security

To mitigate risk and ensure compliance, business leaders must become aware of how data and information move in, through and out of the organization. Data refers to individual numbers, statistics or facts, while information is the result of interpreting that data with context, organization, and purpose. Raw data isn't meaningful; it must be processed or structured to have an impact on the business. In a data breach, cyber criminals use data as a means to gain entry into an organization's systems. In an information breach, in which the accessed files have meaning and value, the impact on the organization is often far greater.

Understanding what data and information you need to keep, and how you can improve the way it is managed, reduces risks and protects you from scrutiny. Establishing information governance standards enables ongoing information confidentiality, integrity and availability.

When considering cybersecurity, unstructured data is often the low-hanging fruit cyber criminals will target to gain access to deeper systems. Identifying and securely disposing of redundant, obsolete and trivial data reduces potential exposure.

Similarly, transactional and inbound information like emails, faxes, mail, web form submissions, document scans, and e-commerce must be received and scanned for potential threats. Integrating information with secured, automated workflows on centralized platforms helps ensure data is safely managed and stored. It also assists with information management and tracking to ensure regulatory and industry compliance. Outbound information, whether distributed to customers or shared through third-party partners, should also be securely handled, encrypted and tracked.

Solution considerations to enable information security in business processes

- Enterprise Content Management (ECM)
- Process Automation
- Information Governance Services
- Cloud hosting

Data security should be addressed with sophisticated encryption, cloud hosting for rigorous centralized management, ransomware prevention and mitigation security, secured data backups and recovery plans, and compliance assessments. Organizations subject to PCI DSS, PII, PIPEDA, HIPAA, FINRA, FERPA, GDPR, CCPA, or FFIEC mandates — or needing to meet compliance requirements that adhere to the HITRUST framework or other corporate security policies — benefit from Ricoh's compliance-centric solutions and professional services.

Layer 3 – Device security

Protecting any type of device — printers, laptops, desktop PCs, smartphones, tablets, wearables, fax machines, or any connected device — from harmful, unauthorized or malicious activity is a critical layer of security. In some industries, compromised IoT devices can cause significant societal or environmental harm. Hybrid work has also led to a greater number of endpoints from remote devices, which has increased the possibility of data breaches exponentially. Devices are also a means to both receiving and delivering inbound and outbound information, so secured connections and practices are a must.

Potential threats can include:

- Malicious access to networks
- Tapping into and alteration of information over the network
- Information leaks from storage media

Unauthorized access via a device's operation panel

- Improper access through fax telephone lines
- Breach access via IoT devices
- Information leaks via hardcopy
- Security policy breaches due to carelessness

Superior technology, diligence, and knowledge are essential, requiring a deep understanding of how to tackle potential issues caused by vulnerabilities in your devices, the data they process, and the networks to which they connect.

At Ricoh, we focus on several methods:

- Device, user and network authentication
- Data encryption
- Remote device management
- IoT management and intrusion detection

Best practices, including firmware and driver management, digitally signed firmware, disabling unused protocols and services, fax line security, simplifying device management with software, meters and alerts, and @Remote.NET.

Ricoh also offers a variety of sustainable devices and services, from materials, capabilities and return programs, among other **ESG offerings**. Not only do sustainable methods help meet environmental goals but they are also designed with secured technology and programs in mind.

Solution considerations to enable secured devices

- Documentation
- Support services
- Intelligent Print (managed print services)
- Smart Lockers
- Data encryption and multi-factor authentication
- IoT Command Center

Layer 4 – Network security

Organizations operate within a borderless world of work, requiring a seamless and secured experience anywhere. As employees access the network and applications from any location or device, attack surfaces multiply while cyber threats are on the rise. Even the smallest crack in a network's defenses can bring serious consequences for the business.

Ricoh offers a robust portfolio of expert IT services and solutions that enable a unified and resilient infrastructure that serves as the backbone for all operations. The main checkpoints for system security processes are:

- Perimeter security
- Network security
- Endpoint protection

Being prepared starts with embedding intelligent cybersecurity measures into your core business processes and ensuring rigorous management by cybersecurity experts. With labor shortages in many industries, Ricoh's expert-driven cybersecurity services and solutions can help you build resilience, understand and manage your vulnerabilities, and enable you to grow with confidence.

Solution considerations to enable secured systems and network

- Perimeter: firewalls, identity and authentication management and penetration testing
- Network: vulnerability assessments with Ricoh IT Services
- Endpoint: anti-virus software, web filtering and mobile device management
- Managed Cybersecurity Services
- Managed IT Infrastructure

Layer 5 – Application security

While software is designed to accelerate efficiency and productivity (often leading to sustainable business practices with data-driven insights and analytics), it can also pose risks. Embedded software applications, operating systems, and software running as cloud services can be potential targets for remote attacks.

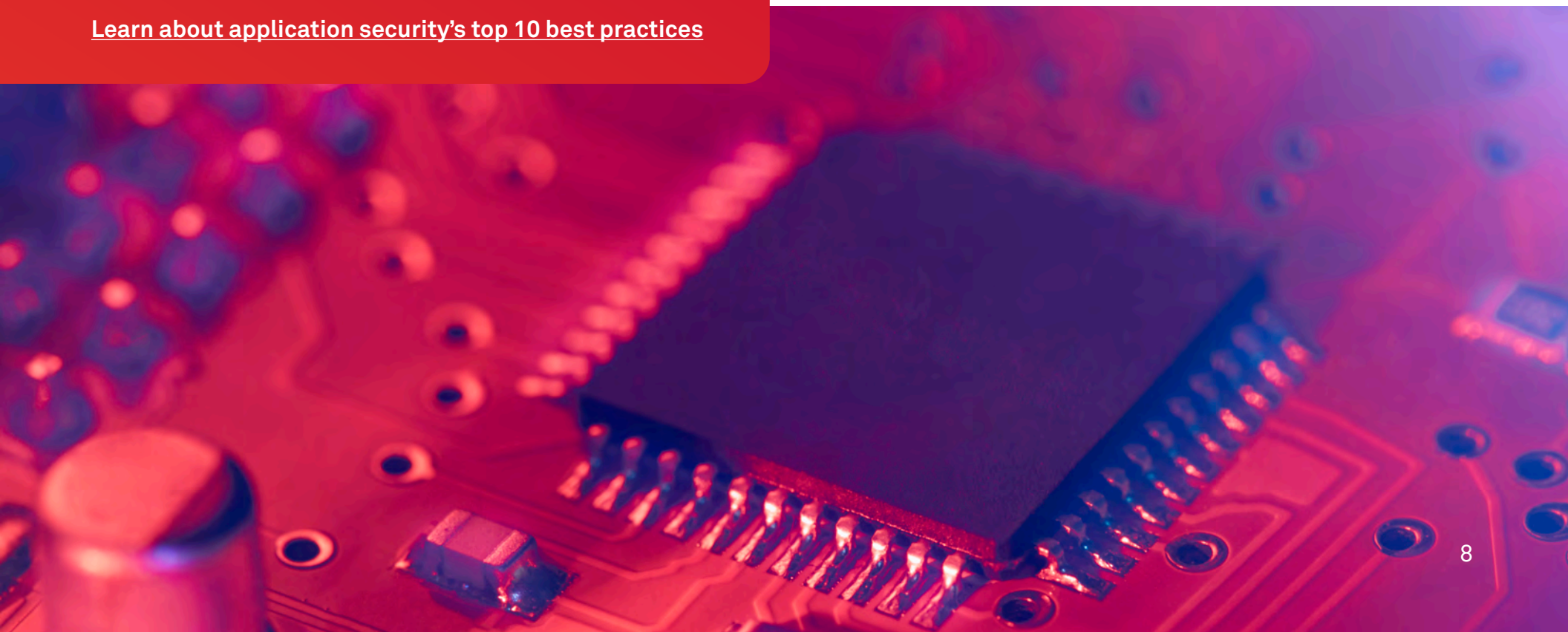
Ricoh provides various software and embedded solutions for IT systems, business process management, print management and more, designed with security in mind. Therefore, firmware and applications that run on Ricoh devices undergo rigorous review and must be compatibility certified and digitally signed by Ricoh in addition to many other security factors.

Ricoh's expert developers can help modernize and better integrate legacy applications to enhance performance, security and compliance. We explore workplace challenges in depth, co-innovating with our customers to build and deliver optimal AI-based solutions that deliver value while ensuring data is secured.

Solution considerations to enable secured applications

- Microsoft 365

Learn about application security's top 10 best practices



Ricoh's security commitment

Whether you're stuck in a data deluge, work in a highly regulated industry, lack resources or experience, or want the assurance of utilizing highly secured services, software, and devices, we aim to gain your trust by having the highest security standards in the industry. Our goal is to stay ahead of cyber criminals — and if they do encroach into our systems, we have a plan and systems in place to mitigate a breach.

Our depth of experience and multi-layered approach can be leveraged across your organization from strategy, devices, software, services, support, training, and more. Let us help you in your digital transformation journey — every day, we work with our customers as they achieve security-enabled business goals such as compliance, brand trust, innovation, business continuity and sustainability.

Ricoh, a trusted partner

At Ricoh, we're empowering our customers to respond to our changing world with actionable insights. We believe having access to the right information translates to better business agility, more human experiences, and the ability to thrive in today's age of hybrid and borderless work. Through our people, experience, and solutions, we create a competitive advantage every day for over 1.4 million businesses around the globe. To us, there's no such thing as too much information.

Are there any areas in your organization that need a security assessment?
Visit **Ricoh-usa.com** or **contact** a Ricoh security expert today. To read our comprehensive Ricoh Essential Security Guide, **download the PDF**.

RICOH
imagine. change.

Ricoh USA, Inc., 300 Eagleview Blvd, Exton, PA 19341, 1-800-63-RICOH.