BEST PRACTICE
CYBER IMMUNITY 2022

ARC White Paper
June 2022

Kaspersky has made available the highly anticipated KasperskyOS, a secure-by-design operating system based on microkernel architecture that is perfectly suited for network devices, industrial control systems and the internet of things.

Cyber Immunity can be the foundation to unleash secure digital transformation in the industrial sector.

By Thomas Menze
Senior Consultant

CONTENTS

Executive Overview

The Internet of Things (IoT) offers an enormous economic advantage for the industrial sector and the development of related services. For example, reduced downtimes of machines and facilities, or autonomously running processes.

While cybersecurity is about software and its implementation, cybersecurity for IoT adds another layer as the cyber and physical worlds come together.

IoT solutions – from remote monitoring, predictive maintenance, energy consumption and management, and smart buildings, to connected products and customer technologies such as mobile apps – optimize operational complexity, cost, and time to market.

Technology experts and analysts predict even wider use of IoT devices and apps in the future, which will naturally be accompanied by the further development of IoT devices, services and apps. This leads to more and more companies wanting to be part of this development. However, many enterprises implement IoT solution strategies conservatively because IoT security concerns are very real. IoT deployments result in unique new security, privacy and compliance challenges for enterprises worldwide.

While cybersecurity is about software and its implementation, cybersecurity for IoT adds another layer as the cyber and physical worlds come together. Many maintenance and operational scenarios in IoT use end-to-end connections so users and services can interact with data. However, companies looking to leverage the efficiency benefits of IoT, such as predictive maintenance, should be aware of what IoT security standards must be met (e.g. IEC 62443 or ISO 27000), as these operational technologies are too important to ignore intrusions, emergencies or other threats.

Cyberattacks against OT Infrastructure

The frequency and sophistication of successful OT cyberattacks should be a warning to asset owners, network operators, and cybersecurity teams. This warning also applies to both IT and OT domains. Uncoordinated defenses from the edge to the cloud pave the way for attacks on production equipment. The multitude of automation components from different manufacturers makes it difficult for plant operators to keep track of cybersecurity in OT networks. Occupational safety, avoiding environmental hazards, and trouble-free operation are the goals of cyber protection most often at the forefront of operators' minds. To this end, they have always relied on protection methods that originated in traditional IT and have been modified for OT applications. But the rapid growth of edge to cloud solutions is forcing users to rethink their security approaches. To proactively secure mission-critical OT, enterprises must consider the following when planning cybersecurity strategies for 2022 and beyond:

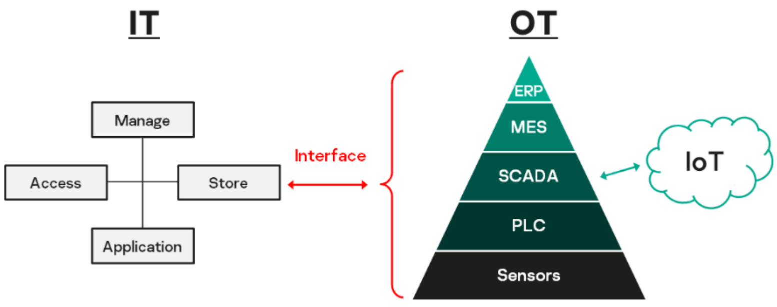
- Design of the security concept
- Levels of protection to be achieved for specific parts
- Maintenance of the security concept over the life cycle
- Ensuring the effectiveness of the security concept

and more.

The evolution towards Industry 4.0 with its focus on process automation and real-time data collection and exchange plays a paramount role. This existing infrastructure is ripe for new attacks on PLC, ICS, OT, and IoT systems that are no longer proprietary but still accessible via the internet. With IT/OT convergence, networked control systems now merge with IT-connected enterprise networks, leading to additional security risks from cross-contamination of LAN, internet, and network traffic control.

The issue is that in most OT networks, cybersecurity is limited. Typical security measures such as virus scanning, endpoint protection, or anomaly detection are of little help because the multitude of IoT components and network structures are difficult to patch and protect effectively in practice.

That is why a strict separation between IT and OT has not existed for a long time. This separation has been united in many places, and not just in the context of the digital transformation. Machines have had remote maintenance access for a long time, where the manufacturer can carry out maintenance remotely. Remote maintenance is the best way to achieve short response times to problems in a cost-effective and timely manner. But adaptions in corporate networks continue to change, driven by digital transformation. Now the aim is to create even more flexible and error-free production.



Source: Kaspersky

An overview of how OT infrastructure must be increasingly networked to achieve digital efficiency is shown in the image on the left. All levels of the automation pyramid are linked with IT in many cases, and more and more IoT networks are also being integrated into automation. Therefore, the attack surface of the automation pyramid continues to increase.

Industry Cybersecurity Countermeasures

Asset owners are using new tactics to take advantage of digital IoT capabilities to increase efficiency. One example is the NAMUR Open Architecture (NOA) concept. It uses non-reactive communication between IoT networks and process automation components. Thus, digital methods are used to increase efficiency, but by using a second communication channel, digital sensor data is separated from traditional process automation. NAMUR describes this concept in NE 175 as follows:

> "The NAMUR Open Architecture (NOA) aims to make production data easily and securely usable for plant and asset monitoring as well as optimization.
>
> Smart sensors, field devices, mobile devices and the ubiquitous use of IT equipment are generating more and more data that is often difficult to access within the classic NAMUR automation pyramid. NOA will change this by transmitting this data over a second communication channel without affecting the widely accepted advantages of traditional automation structures and with no impact on the automation system."

Source: NAMUR

NAMUR is a large interest group in the process automation industry. NAMUR committees develop safety concepts like these in collaboration with universities. Not every production company can define or implement a concept based on its own requirements. The development of a proprietary secure communication concept requires a rethinking of security principles based on the availability, integrity and confidentiality of OT priorities exactly in this order.

It is certainly helpful to use a zero-feedback and manipulation-proof concept for IoT communication right from the start. This reduces the security efforts of IoT suppliers and gives users the freedom to use IoT to increase plant efficiency.

Industry 4.0 Requires the Transformation of OT Cybersecurity

It is no surprise that the growth of cloud computing, APPs and infrastructures is rapidly increasing in complexity and the number of providers. Traditional scanning and patching methods can no longer efficiently secure complex cloud structures.

Outlook

Cybersecurity in process automation has reached a critical point. On the one hand, systems need to be operated as efficiently as possible to ensure the competitiveness of companies. On the other hand, the use of IoT and cloud infrastructure poses a security risk.

Cybersecurity for OT and cloud networks needs to be transformed. In the industrial sector, the concept of Industry 4.0 means digital transformation. For automation technology, this statement is correct, but in terms of cybersecurity, the transformation has yet to take place. What could this transformation look like for cybersecurity? Perhaps it is the transition from cybersecurity to Cyber Immunity. Here, Cyber Immunity is defined as technology that protects against known methods of attack. In addition, protection against unknown attacks is also implemented for the future.

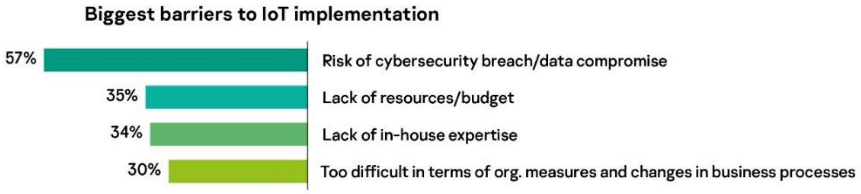
The Kaspersky Global Corporate IT Security Risks Survey (ITSRS) is a global survey of IT workers. A total of 4,303 interviews from businesses with more than 50 employees were conducted across 31 countries in May-June 2021.As concerns cybersecurity impacts and the use of IoT, the ITSRS report provides an insight into IoT specifics.

- In 2021, 53% of organizations abandoned new business projects due to an inability to address cybersecurity risks, and 74% faced a situation where there was no appropriate security solution.
- 64% of organizations already maintain or use IoT solutions.
- 52% of organizations are worried about collecting big data from IoT devices because of the risk of cyber sabotage and espionage.
- However, the risk of a cybersecurity breach is the biggest concern for 57% of organizations planning to implement IoT.

When it comes to cybersecurity risks, no two companies and applications are alike. Effective cybersecurity must be adapted to the threat situation and requires a joint response from all stakeholders. Cyber protection is not a product you invest in once and forget about. It is an ongoing process.

Despite the increasing adoption of IoT, more than half of companies surveyed are concerned about cybersecurity and data integrity when implementing IoT (57%). Lack of resources or budget constraints are cited as a second reason (35%).

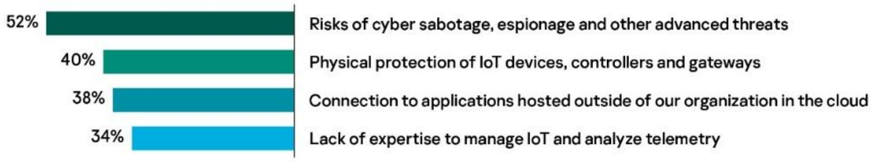
In terms of different industries, 53% of companies in the industrial sector are concerned about security breaches and data compromises, followed by a lack of in-house expertise (35%). The utilities sector is similarly concerned, with 50% and 44%, respectively.



IoT creates a host of new security risks and challenges for devices, platforms and operating systems, their communications, and even the systems they are connected to (e.g., using IoT devices as a point of attack).

Companies surveyed had concerns about collecting large volumes of data from IoT devices because they see a risk of cyber sabotage, espionage, and other advanced threats (52%).

Key concerns for big data in IoT



The Call for Cyber Immunity

To respond to IoT security challenges and support companies using practical cybersecurity solutions, new solutions must be considered.

Efforts are underway to standardize the development of IoT platforms to make them more secure. Such initiatives are driven by associations such as the Institute of Electrical and Electronics Engineers (IEEE) and European Telecommunications Standards Institute (ETSI).

There are also recommendations for organizations on how to build secure IoT systems or assess the state of existing IoT solutions, such as the Industry IoT Consortium's "IoT Security Maturity Model." It guides organizations through processes to help them take security action.

General recommendations for IoT security include the use of encryption and password policies, network segmentation, and firewalls and special protection for cloud infrastructures to which IoT devices connect. These practices are recommended for all critical technology systems.

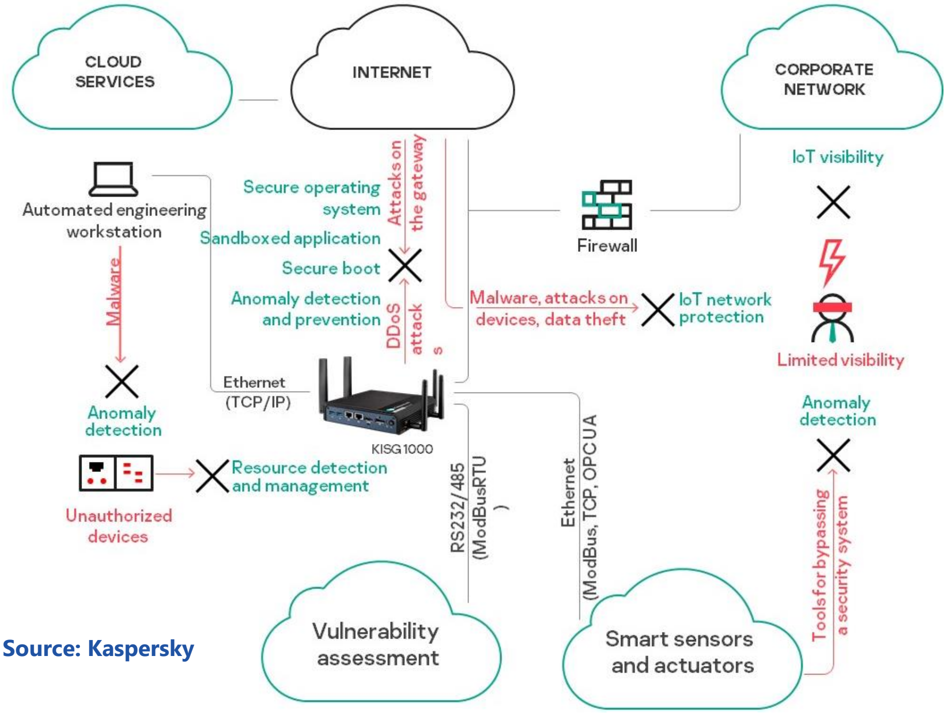
However, there is a unique approach to IoT security called Cyber Immunity, that we have already mentioned before. Cyber Immunity does not focus on eliminating potential vulnerabilities, but on creating conditions where it is impossible to exploit them and affect how a system functions. So even if an application is attacked, it has no impact on the reliable operation of the platform.

This can be achieved with a dedicated operating system and platform development methodology. Our operating system uses a microkernel architecture with only a few thousand lines of code, which eliminates vulnerabilities and reduces the attack surface. This software, with a minimal number of trusted components in the operating system, was developed by Kaspersky and is called KasperskyOS.

KasperskyOS was developed according to the best practices for secure software and includes MILS (Multiple Independent Levels of Security) architecture. This ensures that attacks cannot compromise the system's functions.

So how can KasperskyOS help ensure the cybersecurity of IoT? It can become the basis for Cyber Immune gateways. These gateways are the connecting elements on the edge between the OT (sensors/actuators) and IT (internet) worlds, with all data flowing through them. Therefore, it is possible to protect the infrastructure and its data on the innately protected gateway level.

The typical IoT infrastructure using a KasperskyOS-based Cyber Immune gateway looks like this (on the example of Kaspersky IoT Secure Gateway 1000):

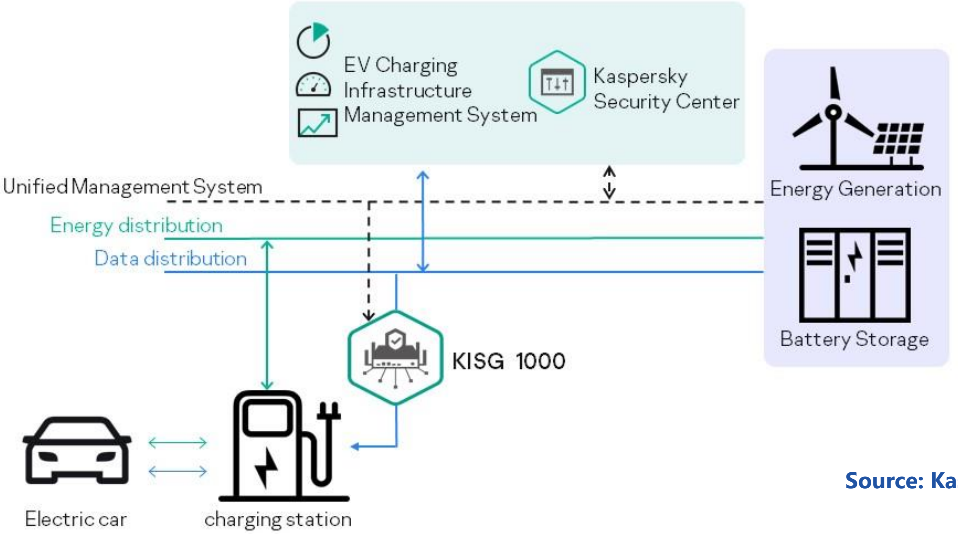


Source: Kaspersky

Best Practice: Electromobility Charging Station

At one point, automation suppliers patched security vulnerabilities in electric vehicle charging stations that could lead to denial-of-service (DoS) attacks.

Suppliers fixed a total of 13 flaws, including three critical vulnerabilities. Charging points are installed on private property, at public parking lots, and for on-street charging. Three charging station product ranges were affected: City, Parking, and Smart Wallbox.



Source: Kaspersky

Exploitation and impact

Charging point owners who failed to download the firmware update "may risk potential unauthorized access to the charging station's web server, which could lead to tampering of the charging station's settings and accounts," they were warned.

Such manipulations could lead to things like denial-of-service attacks, which could result in the unauthorized use of the charging station, service interruptions, and failure to send charging data records to the monitoring system.

Vulnerabilities could be exploited remotely if stations were connected directly to the internet as part of their configuration. Commercial charging infrastructure typically consists of hundreds of chargers, so if an attacker gets network access to them, they can take over all of them. To harden the charging point, it was recommended to change the charging station's internal communication port, which required disassembling the charging station enclosure, or in the case of connected stations, the network of the charging station's monitoring system.

As electric vehicle chargers continue to grow in popularity, it is likely that further serious vulnerabilities will emerge. We can expect the manipulation of charging records or settings to overcharge or undercharge vehicles, and the theft and misuse of charging credentials. In the worst-case scenario, attackers can even find ways to impact the electrical grid.

This is an example of how important it is or will become to secure IoT components with a system that protects against known and unknown cyberattacks. The network and backups of critical infrastructure systems require these protection mechanisms. Here KasperskyOS can be used to ensure effective protection against vulnerable components.

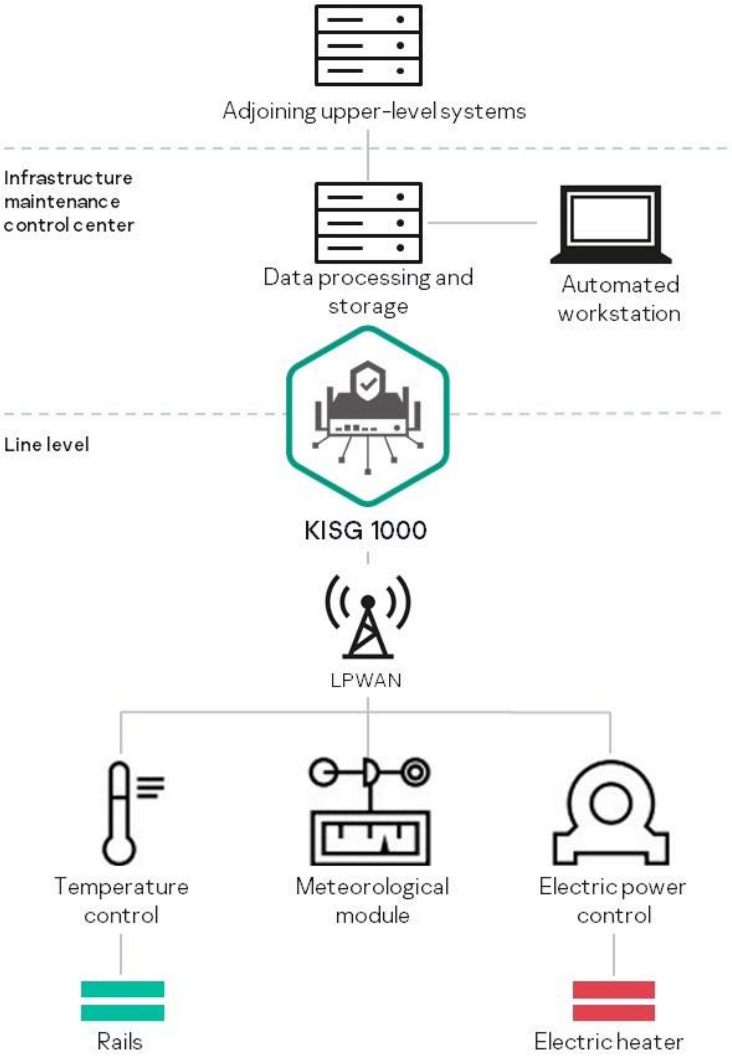
Best Practice: Railway Switch Heating

Railroads are an essential mode of transport and need cost-effective methods to control the use of its resources. To target the reduction of energy demand, an intelligent switch heating IoT system was introduced. Heating is only switched on when the system considers the possibility of freezing, taking into account various environmental parameters received via smart sensors.

A project this complex cannot be carried out without cybersecurity. Railway switch heating systems are connected to the internet and therefore especially vulnerable. Rail traffic is a part of critical infrastructure, so a successful cyberattack would have disastrous consequences. For example, if the smart switch heating system does not recognize weather conditions properly because a cybercriminal tampered with its configurations, the rails may ice up and put all rail traffic at risk.

The KasperskyOS-based Kaspersky IoT Secure Gateway 1000 was installed on the border between the OT and IT levels. Innately secure thanks to Cyber Immunity, it helped ensure the integrity of signal processing without requiring a great deal of maintenance or configuration. Cyberattacks on the gateway were rendered unsuccessful. The same applies if cybercriminals try to manipulate the data from the weather sensors.

Using KISG 1000, the system will stay reliable, properly detecting weather conditions and automatically heating switches even in an aggressive environment.



Source: Kaspersky

Conclusion

Digitalization combines information technology (IT), traditional operational technology (OT) and intellectual property (IP) to boost industry competitiveness.

That is why the merging of OT, IT and IP is taking place in the manufacturing industry. But it takes a long time for most companies to fully accomplish. Thus, we can observe how an entire industry is slowly moving towards Industry 4.0 by replacing equipment piece by piece. Unfortunately, this transformation brings about a number of new cyberthreats and risks.

With the implementation of connected production, digital transformation presents a new cyberthreat profile. While Industry 4.0 presents an ideal picture of production that supports companies in becoming more competitive and efficient, the necessary IT security measures remain unclear.

Overall, IT security must become a matter of course. Not in the sense of running in parallel, but rather being considered from the very start. ICS systems have lifetimes of more than 30 years. New cybersecurity concepts such as Cyber Immunity are crucial here. A system that is innately protected against current and future cyberthreats is indeed a very practical method. Cyber Immunity can be the new foundation for how digital transformation can be implemented more securely.

To this end, OEMs and other technology market leaders are seeking partnerships with cybersecurity vendors to develop secure-by-design products and make security a key differentiator as part of their solutions. For example, to protect industrial and other IoT environments, Kaspersky has partnered with Adaptive Production Technologies to develop Cyber Immune KasperskyOS-based gateways. Capable of integration with Siemens MindSphere, IBM Bluemix, Yandex IoT Core and other cloud platforms, Kaspersky IoT Secure Gateways are reliable tools for digital transformations, protecting the IoT and its data, and being innately protected themselves.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Kaspersky technologies and services provide cybersecurity to over 400 million users, and over 250,000 corporate clients to protect what matters most to them.

Learn more at: https://www.kaspersky.com/

About Kaspersky Cyber Immunity™ and KasperskyOS

Cyber Immunity is an IT system's "inherent" protection — its ability to withstand cyberattacks without any additional (applied) security tools. The overwhelming majority of types of attacks on a Cyber Immune system are ineffective and cannot affect its critical functions in the usage scenarios specified at the design stage.

Kaspersky devised the Cyber Immune approach to creating IT solutions and developed its own KasperskyOS microkernel operating system as a platform for building Cyber Immune products. Cyber Immunity can be achieved by using KasperskyOS and following Kaspersky's special methodology when creating solutions.

Kaspersky provides the KasperskyOS platform and development methodology, and also develops Cyber Immune products in collaboration with its technology partners. Its portfolio includes a product line of IoT gateways to operate in industrial, smart city and other business environments, a solution for building managed and functional infrastructure for thin clients, a specialized SDK to build safe and secure electronic control units (ECU) in automotive projects, and other products.

Learn more at: https://os.kaspersky.com/
Contact us: KasperskyOS_Info@kaspersky.com

About Adaptive Production Technologies (Aprotech)

Adaptive Production Technologies LLC is a subsidiary of Kaspersky that helps enterprises efficiently and securely complete their own digital transformation 4.0. This transformation is facilitated by the company's cutting-edge Cyber Immune IoT gateways that enable data transport in end-to-end digital services developed together with partners to accomplish the business tasks of clients. The assistance by Aprotech, including consulting and audit, R&D and training, streamlines the cybersecure transition to new technologies.

Learn more at: https://www.aprotech.online/

Analyst: Thomas Menze

Acronym Reference:

ERP	Enterprise Resource Planning
IP	Intellectual Property
IoT	Internet of Things
IT	Information Technology
KISG	Kaspersky IoT Secure Gateway
MES	Manufacturing Execution System
NOA	NAMUR Open Architecture
OT	Operational Technology
PLC	Programmable Logic Controller
SCADA	Supervisory Control & Data Acquisition

Founded in 1986, ARC Advisory Group is a leading technology research and advisory firm for industry, infrastructure, and cities. ARC stands apart thanks to our in-depth coverage of information technologies (IT), operational technologies (OT), engineering technologies (ET), and associated business trends. Our analysts and consultants have the industry knowledge and first-hand experience to help our clients find the best answers to the complex business issues facing organizations today. We provide technology supplier clients with strategic market research and help end user clients develop appropriate adoption strategies and evaluate and select the best technology solutions for their needs.

This research has been sponsored in part by Kaspersky/ Aprotech. However, the opinions expressed by ARC in this paper are based on ARC's independent analysis.

You can take advantage of ARC's extensive ongoing research and the experience of our staff members through our Advisory Services. ARC's Advisory Services are specifically designed for executives responsible for developing strategies and directions for their organizations. For membership information, please call or write us, or visit our website:

ARC Advisory Group, Three Allied Drive, Dedham, MA 02026 USA • 781-471-1000 • www.arcweb.com