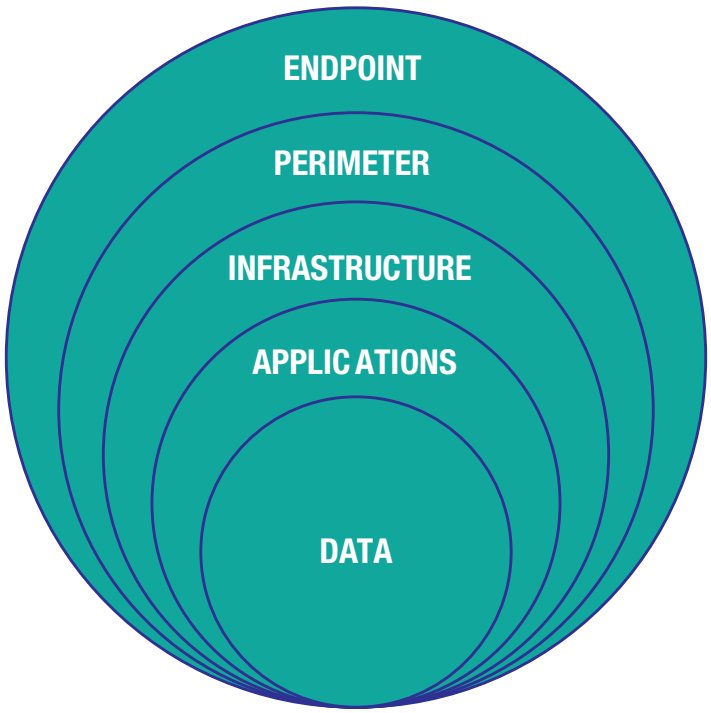
EVERY LEVEL OF CORPORATE DATA FUNCTION NEEDS SECURITY EVALUATION

EVERY LEVEL OF CORPORATE DATA FUNCTION NEEDS SECURITY EVALUATION

The vastness of today's global business community creates the confusion and dis-coordination that cyber criminals look for in their targets. Companies with complex supply chains, international vendors, and worldwide markets may have thousands of vulnerabilities that invite these hackers to send in malware, run phishing trips or shut down entire divisions with ransomware.

The security experts at IIS have analyzed the technological portals through which these miscreants enter the company sphere. These portals can be found anywhere in the enterprise-wide digital system, from data storage facilities and networking banks through to the virtualized global structure and enterprise-specific software and hardware. With this knowledge, the IIS security experts develop and perfect the impenetrable security strategies needed to thwart the criminals at every level.



LAYERS OF THREATS

In today's environment, each layer is vulnerable to cyberattacks and must be secured. If a layer is compromised, it can impact other layers. Security mitigation must address all points of access.

DATA

Information is the lifeblood of every enterprise; securing that data means securing the company's future. Data has its own vulnerabilities and needs to be protected, while at rest and in motion, through deployment of a defense-in-depth security approach. One option is to encrypt the data as it comes into the system. If data is stolen because of a breach in another layer, it is of little or no value to the thief as it is in an encrypted form. The challenge: deploying a security approach for corporate data that is accessed daily, from perhaps hundreds of portals, and by potentially hundreds of authorized users.

APPLICATIONS

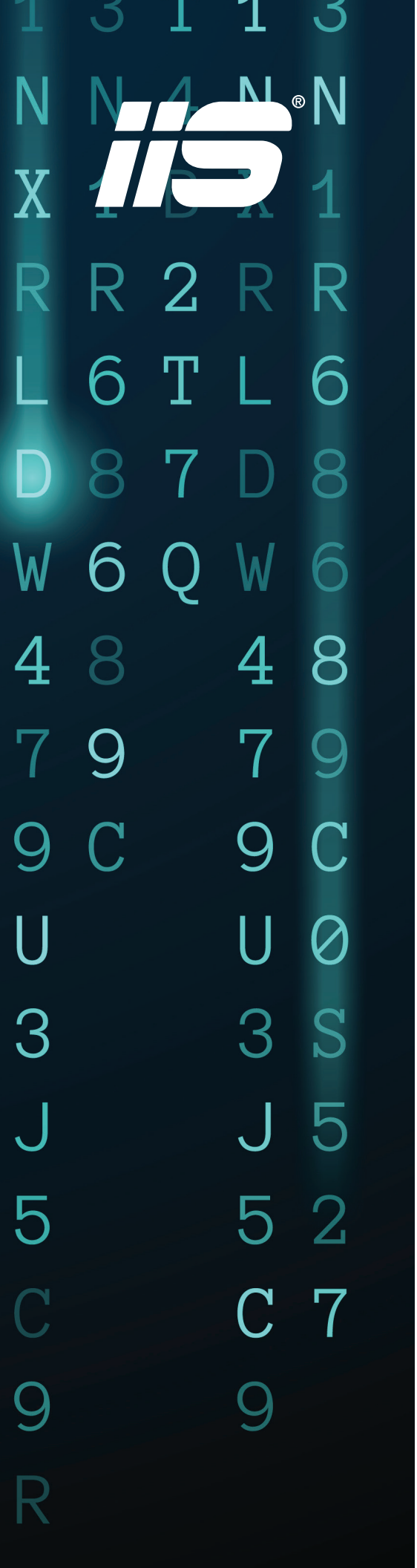
Both professional and amateur coders develop today's applications, many of them are not aware (or do not care) that their code may contain dangerous flaws that can compromise user devices or data. The "BYOD" (Bring Your Own Device) trend exacerbates the issue because each device may be carrying the small bit of malware that takes down the whole company.

INFRASTRUCTURE

Today's digital infrastructure, the communication pathway of all industries, should be secure, flexible and accessible to accomplish each day's goals. Insider threats by unscrupulous or disillusioned employees exploit their proprietary knowledge of corporate infrastructure for their personal gain. It is not enough to protect against attacks from outsiders who don't know your system well, you must also protect against some of the people you thought you could trust, people with intimate knowledge and access to your systems.

PERIMETER

Even with myriad perimeter defenses installed, if those security elements are not coordinated and comprehensive, intruders can still creep through the cracks. Understanding how firewalls fail can be critical to preventing the attacks that circumvent them.



ENDPOINT

Endpoint users, including employees, vendors, supply chain operations and logistics, represent entry points into a company's operations and are the most vulnerable and exploitable aspects of the corporate security plan. Companies with exceptional cyber security systems in place can still be affected indirectly by an off-shore provider that has few or no such defenses in place.

IDENTIFICATION OF RISKS CLARIFIES SECURITY NEEDS.

The purpose of cyber security systems is to detect, deter and mitigate the risks of loss caused by digital crime. The security experts at IIS take a methodical, collaborative approach to identifying and solving digital security concerns for their national and international clients.

The initial, thorough assessment of existing systems and policies often reveals vulnerabilities that are so new that the client company is not yet aware that they exist.

IIS customers are actively engaged in the planning of their evolving security strategy, bringing their proprietary knowledge into the design itself. During and after installation, configuration and the testing phase, the risks facing the company and the protections secured by the new security strategy are explained in detail to corporate IT management.

At IIS, the knowledge base and technology are always current, so their customer's systems are also always current. IIS's innovative and responsive data management tools - storage, networking, and security among others - provide the insight needed to proactively structure every company's IT to meet today's needs while anticipating tomorrow's. IIS experts are available to talk to you now; they will help you find the answer to your cyber security question.

IIS can help your enterprise construct its digital security systems for today and for tomorrow.

odiaz@iisl.com

877-704-4001

http://www.iisl.com/