UNISOL TECHNOLOGIES
EST. 2016

UNISOL CYBERSEC

UNISOL TECHNOLOGY

UNISOL CLOUD

2026 Digital Security Guide for Businesses

Assess, Protect & Strengthen Your Business

CYBERSECURITY STARTS WITH A PREPARED INFRASTRUCTURE

LCybersecurity is not just about installing antivirus software or having a firewall. A truly protected business needs technology infrastructure that is up to date, continuously monitored, and prepared to respond to threats.

From the devices your employees use to applications, networks, backup systems, and cloud services, every component is part of your organization's attack surface.

That is why, in addition to identifying common threats, this eBook will help you assess key elements of your technology infrastructure and identify opportunities to strengthen them. It will also guide you through the latest cybersecurity trends, providing practical tools and recommendations to help keep your business secure in 2026 and beyond.

¿What Should You Assess?

- **IT Infrastructure:** Are your devices, networks, and systems up to date and protected?
- **Cybersecurity:** Do you have multiple layers of protection against threats?
- **Data & Backups:** Could you recover your information if an attack occurred?
- **Users & Access:** Does each employee have only the permissions they need?
- **Cloud:** Are your cloud services properly configured and protected?
- **Business Continuity:** Could your business continue operating after an incident?

A secure business doesn't just react to threats. It prepares before they happen.

En un mundo cada vez más digital, la ciberseguridad se ha convertido en un pilar fundamental para proteger los datos y activos de las empresas. A medida que las amenazas cibernéticas evolucionan, también deben hacerlo las estrategias y herramientas de protección.

Why Is Cybersecurity Important for Your Business?

Why is it critical?

Cyberattacks don't just affect your systems—they can also damage your reputation.

For example, attacks against healthcare organizations can compromise sensitive patient data and disrupt operations, resulting in delays in delivering medical services.

In retail stores and hardware businesses, an incident can disrupt sales, inventory, and payment systems.

Professional services firms may face the exposure of confidential client information and internal documents.

In manufacturing, an attack can bring production to a halt and result in significant financial losses.

These incidents demonstrate how a lack of cybersecurity preparedness can have operational, financial, and reputational consequences, regardless of a company's size or industry.

CHAPTER 1: EMERGING CYBER THREATS FOR 2026

Types of Cyber Threats

- **Malware & Viruses:** Malware, or "malicious software," is a general term used to describe any program or code designed to harm systems. Malware attempts to infiltrate, damage, or disable computers, IT systems, networks, tablets, and mobile devices, often taking partial control of the device.

- **Ransomware:** Ransomware is a type of malware that prevents users from accessing infected devices or systems. Cybercriminals may take control of a device or system by encrypting information, locking the screen, or using other methods. The victim is then extorted and asked to pay a ransom in exchange for restoring normal access to the device or system.

- **Phishing y Spear Phishing:** These techniques manipulate people into providing information, credentials, money, or access to systems. They can appear through emails, text messages, phone calls, fake websites, or impersonation of trusted individuals and organizations.

- **Credential Theft:** Credential theft attacks are designed to obtain usernames, passwords, and other authentication information in order to access business accounts, applications, and systems. Compromised credentials continue to be one of the primary methods attackers use to gain access.

- **Vulnerability Exploitation:** Cybercriminals take advantage of security vulnerabilities in software, applications, network devices, VPNs, and other systems to gain unauthorized access. Keeping systems up to date and applying security patches is essential to reducing this risk.

- **AI-Powered Attacks:** Artificial intelligence enables cybercriminals to create more convincing phishing campaigns, automate attacks, and generate malicious content at a much larger scale. This makes fraudulent attempts increasingly difficult to identify.

CHAPTER 1: EMERGING CYBER THREATS FOR 2026

The Cost of Cyberattacks

A cyberattack can result in much more than an immediate recovery cost.
Businesses may face operational disruptions, lost productivity, system recovery expenses, exposure of sensitive information, customer loss, and reputational damage.

For small and midsize businesses, the impact can be especially significant because they often have more limited IT and cybersecurity resources.
A cyberattack can cost a small business between 3% and 10% of its annual revenue.

That's why prevention, early detection, and having an incident response plan are essential to strengthening business resilience.
Meeting applicable regulatory and compliance requirements not only helps reduce legal and regulatory risks, but also strengthens trust among customers, employees, and business partners.

In Puerto Rico, businesses may be subject to different requirements depending on their industry, the type of data they handle, and the regulations that apply to them.

For this reason, it is important for each organization to evaluate its specific obligations and keep its security practices up to date.

CHAPTER 2: COMPLIANCE REQUIREMENTS IN PUERTO RICO

Complying with privacy and security requirements is not only a legal obligation for certain industries; it is also a fundamental part of a responsible cybersecurity strategy.

Businesses should identify which regulations, laws, and standards apply to their industry, the type of information they handle, and the services they provide. Below are some of the key laws, regulations, standards, and frameworks that may apply to businesses in Puerto Rico, depending on their industry and the data they handle.

- **Puerto Rico Law No. 111-2005**

Establishes requirements related to the protection of personal information and the notification of certain security breaches that may compromise sensitive data.

  - **Recommendation:** Maintain an incident response plan and clear procedures for identifying, documenting, and reporting potential security breaches.

- **HIPAA / HITECH - Sector de Salud**

Applies to certain healthcare organizations and their business associates to safeguard protected health information (PHI).

  - **Recommendation:** Implement encryption, access controls, multi-factor authentication (MFA), monitoring, and periodic risk assessments.

CHAPTER 2: COMPLIANCE REQUIREMENTS IN PUERTO RICO

- **GLBA / FTC Safeguards Rule — Financial Services**

Requires certain financial institutions to implement measures to protect customer information.

  - **Recommendation:** Establish a security program that includes risk assessments, access controls, data protection, and incident response.

- **PCI DSS - Pagos con Tarjeta**

Estándar de seguridad para empresas que procesan, almacenan o transmiten
datos de tarjetas de pago. Es especialmente relevante para comercios que aceptan pagos con tarjeta.

  - **Recommendation:** Protege los datos de pago, limita el acceso y mantén sistemas y aplicaciones actualizados.

- **NIST Cybersecurity Framework 2.0**

Marco de referencia que ayuda a empresas de cualquier industria a gestionar sus riesgos de ciberseguridad mediante seis funciones: **Govern** (Gobernar), **Identify** (Identificar), **Protect** (Proteger), **Detect** (Detectar), **Respond** (Responder) y **Recover** (Recuperar).

  - **Recommendation:** Utiliza el framework para evaluar tu nivel de seguridad y crear un plan de mejora continua.

What Applies to Your Business?

Not every business is subject to the same regulations.
Identifying which requirements apply to your industry is the first step toward developing an effective security strategy.

CHAPTER 3: SECURITY STRATEGIES TO PROTECT YOUR BUSINESS

An effective cybersecurity strategy combines technology, processes, and people. These practices can help reduce risk and strengthen your business's protection.

Zero Trust Security Model

Implementation

Adopt a Zero Trust security model that assumes no entity inside or outside your network is trusted by default.

For example, establish access policies based on the principle of least privilege, requiring every user and device to be authenticated and authorized before accessing critical resources.

Cloud Security

Multi-Cloud Protection

Make sure all your cloud platforms, whether public, private, or hybrid, are properly protected.

For example, use integrated cloud security solutions that provide visibility and control across all environments in which you operate.

Advanced Access Management

Implement Identity and Access Management (IAM) systems to control who has access to which resources.

CHAPTER 3: SECURITY STRATEGIES TO PROTECT YOUR BUSINESS

Continuous Training

Develop Dynamic Training Programs

Create interactive cybersecurity training programs and update them regularly.

An effective cybersecurity strategy combines technology, processes, and people. These practices can help reduce risk and strengthen your business's protection.

CHAPTER 4: INCIDENT RESPONSE & RECOVERY PLANS

Prepare for the unexpected with a structured plan.

This chapter guides you through creating a strong and effective incident response plan. Learn how to conduct exercises, use advanced monitoring tools, and develop recovery strategies that can help you overcome cyber incidents and maintain business continuity.

Building an Incident Response Plan

- **Key Components of an Incident Response Plan**

Include procedures to identify, contain, eradicate, and recover from security incidents.

For example, establish an incident response team with clearly defined roles and responsibilities, along with a communications plan for notifying stakeholders.

- **Response Exercises**

Conduct exercises regularly to test the effectiveness of your plan and make adjustments as needed.

Advanced Monitoring & Detection Tools

- **Using Artificial Intelligence & Machine Learning**

Use these technologies to proactively detect threats. They can identify abnormal patterns and respond to threats in real time, improving the efficiency of your security strategy.

CHAPTER 5: A PREPARED TECHNOLOGY INFRASTRUCTURE

Cybersecurity doesn't begin only when an attack occurs.
A protected business needs technology infrastructure that is prepared to prevent threats, maintain operations, and recover when necessary.
Computers, networks, applications, users, data, and cloud services are all part of the same ecosystem. That's why security must be approached holistically.

What Should a Business Consider?

Infrastructure & Devices

Keeping devices, systems, and applications up to date helps reduce vulnerabilities.

A well-managed infrastructure should include endpoint protection, a firewall, monitoring, and regular maintenance.

It's also important to maintain visibility into the organization's devices and ensure that only authorized users can access them.

Identity & Access

Protecting accounts is just as important as protecting devices. Implement:

- Multi-factor authentication (MFA)
- Individual accounts for each user
- Role-based access
- The principle of least privilege
- Regular permission reviews

CHAPTER 5: A PREPARED TECHNOLOGY INFRASTRUCTURE

Remote Work & Productivity

Remote work requires employees to securely access their tools from different locations.

Productivity and collaboration solutions should have appropriate access controls, email protection, and policies that help keep business information secure.

Cloud & Business Continuity

Cloud services can help businesses improve collaboration, accessibility, and scalability.

However, moving information to the cloud does not automatically mean that it is protected.

Before adopting or migrating to cloud services, consider:

- Who will have access?
- How will we protect user accounts?
- Is MFA enabled?
- How will information be backed up?
- How will we recover data after an incident?
- Can we continue operating if a service becomes unavailable?

A well-planned cloud strategy can become an important part of business continuity and growth.

CHAPTER 5: A PREPARED TECHNOLOGY INFRASTRUCTURE

From Reactive to Preventive

An effective technology strategy moves beyond solving problems after they occur to identifying risks and opportunities before they affect operations.

This requires combining:

Support + Infrastructure + Cybersecurity + Cloud + Business Continuity

When these elements work together, technology becomes more than a resource for solving problems, it becomes a business enabler.

How Prepared Is Your Business?

Use the following self-assessment to identify which areas of your infrastructure, security, and cloud services are already strong and which may require additional attention.

SECURITY CHECKLIST

Below is a practical, scored checklist to help you assess and improve your business's security measures.

Yes= 2 points Partiall= 1 point No= 0 points

IT Infrastructure	
Regularly update systems and software.	
Implement a robust firewall.	
Conduct periodic vulnerability assessments.	
Sensitive Data Protection	
Encrypt data at rest and in transit.	
Implement access control policies.	
Emergency Response Preparedness	
Develop an incident response plan.	
Conduct response exercises.	
Employee Education & Awareness	
Provide regular cybersecurity training.	
Establish a security-minded culture.	
TOTAL SCORE	

0-10= High Risk 11-20= Moderate Risk 21-30= Low Risk

Unified cybersecurity solutions to protect your people, devices, data, and business operations.

UNISOL CYBERSEC

PROVEN SOLUTIONS

1. Strengthen Your IT Infrastructure

To protect your systems, it is critical to have a strong technology infrastructure.

Make sure you:

Keep All Systems & Software Up to Date: Security updates often fix vulnerabilities that attackers could exploit.

Implement a Robust Firewall: A firewall acts as a barrier between your internal network and the outside world, blocking unauthorized access.

Conduct Regular Vulnerability Assessments: Identify and address weaknesses in your systems before attackers discover them.

2. Protect Sensitive Data

Data protection is essential for customer trust and regulatory compliance. Consider the following measures:

- Data Encryption: Protect confidential information by encrypting it both in transit and at rest, so that even if data is intercepted, it cannot be accessed without the appropriate key.
- Access Control: Implement restricted-access policies so that only authorized individuals can view or modify sensitive data.

3. Prepare for Emergency Response

Having an incident response plan is critical to minimizing the impact of a cyberattack.

Make sure you:

- Develop an Incident Response Plan: Establish a clear protocol for handling different types of incidents, from ransomware attacks to data breaches.

- Conduct Regular Exercises: Practice your plan through regular exercises to make sure everyone on your team knows what to do in the event of an emergency.

UNISOL TECHNOLOGIES
EST. 2016

UNISOL CYBERSEC

UNISOL TECHNOLOGY

UNISOL CLOUD

HOW UNISOL CAN HELP

At UniSol, we help businesses turn technology into a competitive advantage. We provide comprehensive solutions covering managed IT services, cybersecurity, cloud, networking, Microsoft 365, technical support, licensing, and technology solutions tailored to each organization's needs. From protecting your systems and data to optimizing your infrastructure, improving team productivity, and keeping your operations connected, we work with you to build a technology strategy that is secure, efficient, and ready to grow.

Ready to Strengthen Your Technology and Take Your Business to the Next Level?

UNISOL TECHNOLOGIES
EST. 2016

UNISOL CYBERSEC

UNISOL TECHNOLOGY

UNISOL CLOUD

¡ACT NOW!

Website
www.unisolpr.com

Phone
939-320-4999

E-mail
info@unisolpr.com

Social Media
@unisoltechnologies

Address
438 Ave. Hostos
San Juan, Puerto Rico 00918