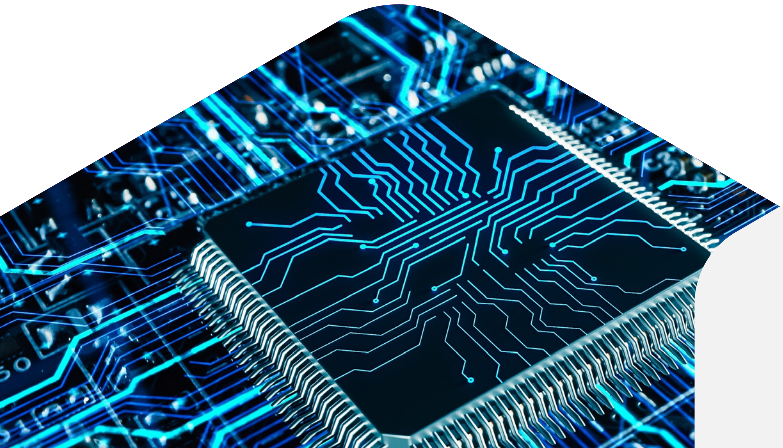
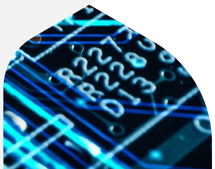
VIATEL
TECHNOLOGY GROUP

Cybersecurity
A Real-World Manual

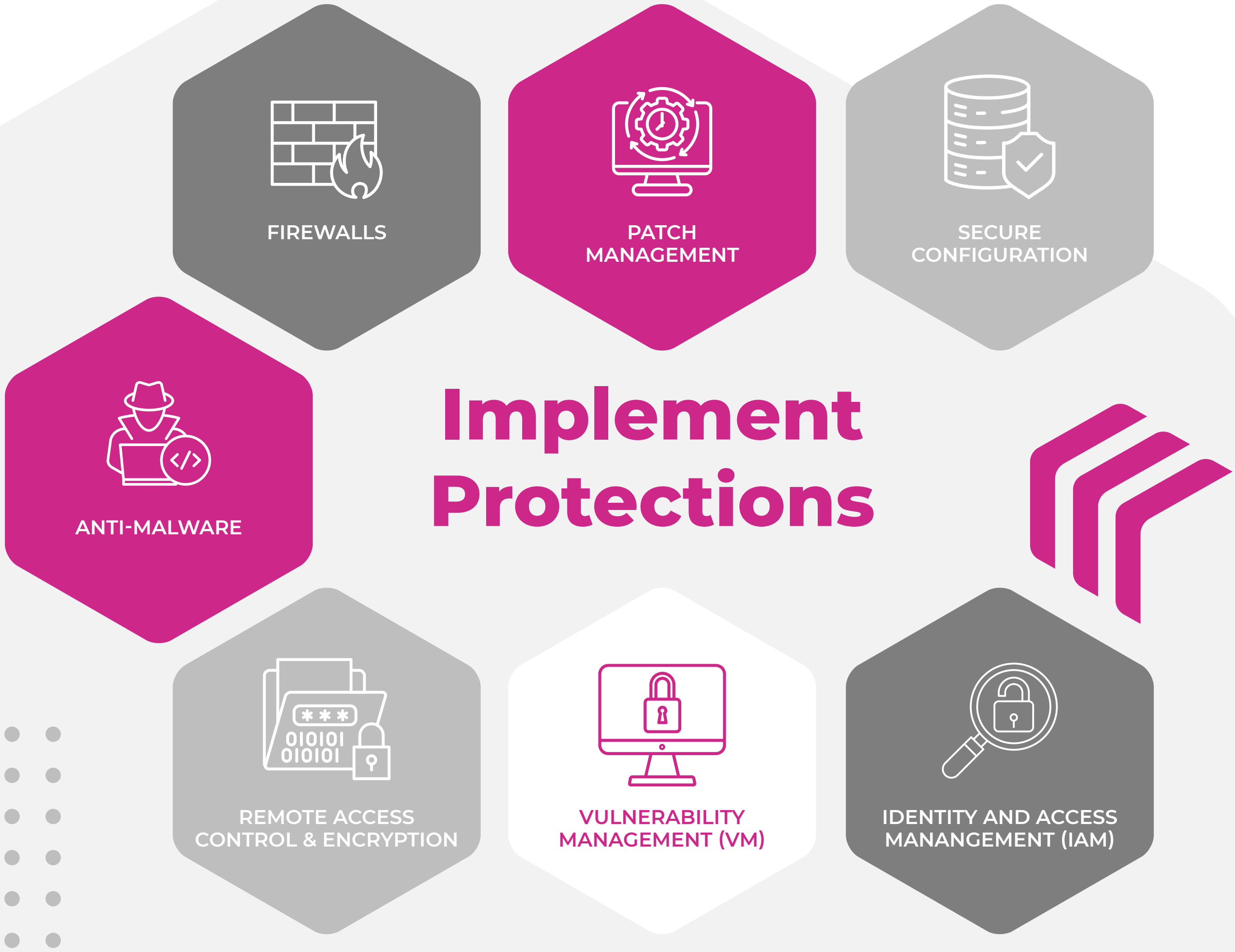




Five Step Fundamentals

1. Implement Protections

Secure your organisation at the technology level by deploying essential protections such as secure configuration, patch management, firewalls, anti-malware, and removable media controls. Implement remote access controls and encryption. Establish a Vulnerability Management (VM) programme to manage vulnerabilities from identification through to remediation. Develop an effective Identity and Access Management (IAM) programme to control access to your information. Prioritise data protection and privacy (both technical and compliance aspects) and manage third parties who have access to or control of your data.



FIREWALLS

PATCH MANAGEMENT

SECURE CONFIGURATION

ANTI-MALWARE

Implement Protections

REMOTE ACCESS CONTROL & ENCRYPTION

VULNERABILITY MANAGEMENT (VM)

IDENTITY AND ACCESS MANANGEMENT (IAM)

2. Understand the Threats

Gain a clear understanding of who might want to attack you, why they would target your organisation, and how they might carry out such an attack. This knowledge allows you to focus your efforts on responding to the most likely threats.

3. Focus on Education and Awareness

Establish a comprehensive education and awareness programme. Ensure all employees, contractors, and third parties can identify a cyberattack and understand their role in defending your business against threat actors.

4. Be Able to Detect an Attack

Develop a security monitoring capability to detect attacks by monitoring activity at various levels within your business. Depending on your industry and available resources, this could range from a basic system that generates and emails alerts when suspicious activity is detected on a firewall, to a 24/7/365 Security Operations Centre monitoring networks, operating systems, applications, and end-users.

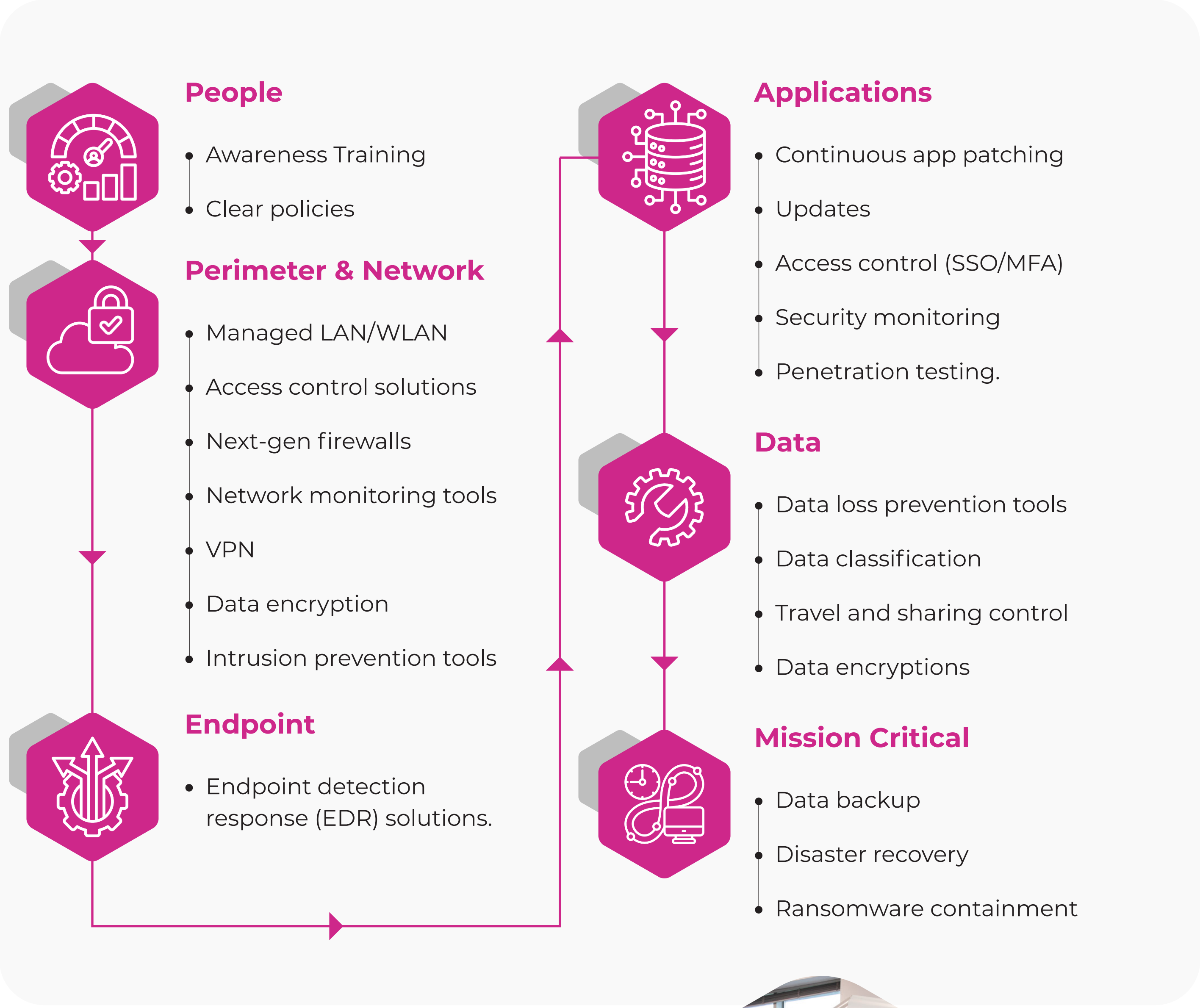
5. Be Prepared to React

Form a formal cyber incident management team trained to follow a documented plan. Ensure this plan is tested at least annually to maintain readiness and effectiveness.

AT A GLANCE

Your Cybersecurity Ecosystem

Cybersecurity is relevant to each and every aspect of your business. Protecting your people, data and infrastructure are critical to your operational resilience and defence against threats. Let's take a look at some of the key considerations you should make for your organisation.



People

- Awareness Training
- Clear policies

Perimeter & Network

- Managed LAN/WLAN
- Access control solutions
- Next-gen firewalls
- Network monitoring tools
- VPN
- Data encryption
- Intrusion prevention tools

Endpoint

- Endpoint detection response (EDR) solutions.

Applications

- Continuous app patching
- Updates
- Access control (SSO/MFA)
- Security monitoring
- Penetration testing.

Data

- Data loss prevention tools
- Data classification
- Travel and sharing control
- Data encryptions

Mission Critical

- Data backup
- Disaster recovery
- Ransomware containment

RANSOMWARE

What Can a Ransomware Attack Look Like?

- A customer receives an email. It looks legitimate, but with one click on a link or one download of an attachment, everyone is locked out of your network. That link has downloaded software that holds your customer data hostage.
- The attackers demand money, but even if you pay, there's no guarantee they won't keep your data or destroy your files.
- Meanwhile, the information you need to run your business, along with sensitive details about your customers, employees, and company, is now in criminal hands. Ransomware can take a serious toll on your business.

How It Happens

Criminals can initiate a ransomware attack in several ways:

- **Scam Emails:** Phishing emails with links and attachments that put your data and network at risk. These emails account for most ransomware attacks.
- **Server Vulnerabilities:** Hackers can exploit weaknesses in your servers.
- **Infected Websites:** Websites that automatically download malicious software onto your computer.
- **Online Ads:** Ads containing malicious code, even on trusted websites.

How to Protect Your Organisation

1. Have a Plan:
How would your organisation stay operational after a ransomware attack? Work with your technology partner to create a plan. Document this plan and share it with everyone who needs to know.

2. Back Up Your Data:
Regularly save important files to a drive or server that's not connected to your network. Make data backup part of your routine business operations.

3. Keep Your Security Up to Date:
Always install the latest patches and updates. Look for additional means of protection, like email authentication and intrusion prevention software, and set them to update automatically on your computer and devices. If using an IT provider, ensure that they provide you with regular reports on patching and service levels.

4. Alert Your Staff:
Teach your staff how to avoid phishing scams and show them common ways computers and devices become infected. Include tips for spotting and protecting against ransomware in your regular orientation and training.

By following these steps, you can significantly reduce the risk of a ransomware attack and ensure your business is prepared to respond effectively if one occurs.

PHISHING

What Can a Phishing Attack Look Like?

- You receive an email that looks like it's from someone you know, such as your IT Director or Branch Manager.
- You receive an email that appears to be from a vendor, asking you to click on a link to update your account.

What You Can Do

It Looks Real: Scammers can easily spoof logos and create fake email addresses. They often use familiar company names or pretend to be someone you know.

Check It Out: Look up the website or phone number for the company or person behind the text or email. Ensure you're contacting the real company and not about to download malware or talk to a scammer.

Talk to Someone: Discussing the email with a colleague might help you determine if the request is genuine or a phishing attempt.

It's Urgent: The message pressures you to act immediately, suggesting something bad will happen if you don't.

What Happens Next: If you click on a link, scammers can install ransomware or other malicious programs that lock you out of your data and potentially spread across your entire company network. If you share passwords, scammers now have access to all those accounts.

Make a Call if You're Not Sure: Pick up the phone and call the vendor, colleague, or client who sent the email. Confirm that they really need the information from you. Use a number you know to be correct, not the one provided in the email or text.

By staying vigilant and verifying the authenticity of such requests, you can protect your business from phishing attacks and maintain a secure environment.

How Phishing Works

You get an email or text that seems to be from someone you know, asking you to click a link or provide your password, bank account details, or other sensitive information.

How to Protect Your Business

Back Up Your Data

Regularly back up your data and ensure those backups are not connected to the network. This way, if a phishing attack occurs and hackers infiltrate your network, you can restore your data. Make data backup a routine part of your operations.

Keep Your Security Up to Date

Always install the latest patches and updates. Look for additional protection measures, such as email authentication and intrusion prevention software, and set them to update automatically on your computers. On mobile devices, you may need to do this manually.

Alert Your Staff

Share this information with your team. Remember that phishing scammers frequently change their tactics, so include tips for spotting the latest phishing schemes in your regular training sessions.

Deploy a Safety Net

Use email authentication technology to help prevent phishing emails from reaching your company's inboxes in the first place.

How to Protect Your Business

CONTROL ACCESS

USE MULTI-FACTOR AUTHENTICATION

SECURE YOUR NETWORK

SAFEGUARD YOUR DATA

Protecting Devices

Whether employees or vendors use company-issued devices or their own when connecting remotely to your network, those devices should be secure. Follow these tips — and ensure your employees and vendors do as well:

- **Change Router Passwords:** Always change any pre-set router passwords and the default name of your router. Keep the router's software up to date; you may need to visit the router's website often to do so.

- **Enable Full-Disk Encryption:** Consider enabling full-disk encryption for laptops and other mobile devices that connect remotely to your network. This protects any data stored on the device if it's lost or stolen, especially if the device stores sensitive personal information.

- **Adjust Smartphone Settings:** Change smartphone settings to stop automatic connections to public Wi-Fi.

- **Update Antivirus Software:** Keep up-to-date antivirus software on devices that connect to your network, including mobile devices.

Connecting to the Network Remotely

Require employees and vendors to use secure connections when connecting remotely to your network. They should:

- **Use WPA2 or WPA3 Encryption:** Use a router with WPA2 or WPA3 encryption when connecting from their homes. Encryption protects information sent over a network so that outsiders can't read it. WPA2 and WPA3 are the only encryption standards that will protect information sent over a wireless network.

- **Use a VPN with Public Wi-Fi:** Only use public Wi-Fi when also using a virtual private network (VPN) to encrypt traffic between their computers and the internet. Public Wi-Fi does not provide a secure internet connection on its own. Your employees can get a personal VPN account from a VPN service provider, or you may want to hire a vendor to create an enterprise VPN for all employees to use.

Maintaining Security

- **Regular Training:** Include information on secure remote access in regular trainings and new staff orientations.

- **Cybersecurity Policies:** Have policies covering basic cybersecurity, give copies to your employees, and explain the importance of following them.

- **Device Security Requirements:** Before letting any device — whether at an employee's home or on a vendor's network — connect to your network, make sure it meets your network's security requirements.

- **Public Wi-Fi Risks:** Inform your staff about the risks of public Wi-Fi.

Training and Tools

- **Unique, Complex Passwords:** Require employees to use unique, complex network passwords and avoid unattended, open workstations.

- **Multi-Factor Authentication:** Require multi-factor authentication to access areas of your network that have sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

- **Separate Guest Wi-Fi:** If you offer Wi-Fi on your premises for guests and customers, make sure it's separate from and not connected to your back office network.

- **VPN for Remote Access:** Consider creating a VPN for employees to use when connecting remotely to the network.

- **Vendor Security Provisions:** Include provisions for security in your vendor contracts, especially if the vendor will be connecting remotely to your network.

EMAIL SECURITY

What can an email scam look like?

A scammer sets up an email address that looks like it's from your business.

The scammer then sends out messages using that email address. Scammers do this to get passwords and bank account numbers or to get someone to send them money. When this happens, you risk losing the trust of your customers and partners.

How to protect your business

Use Email Authentication

When setting up your organisation's email, ensure your email provider offers email authentication technology. This way, when you send an email from your server, the receiving servers can verify that the email is genuinely from you. If it's not, the receiving servers may block the email, hindering any business email imposters.

Keep Your Security Up to Date

Always install the latest patches and updates. Set them to update automatically across your network. Look for additional protection measures, such as intrusion prevention software, which monitors your network for suspicious activity and alerts you if it detects anything unusual.

Train Your Staff

Educate your team on how to avoid phishing scams and recognise common methods attackers use to infect computers and devices with malware. Leverage the expertise of cybersecurity awareness trainers to ensure that your team are well equipped to recognise email threats.

PHYSICAL SECURITY

Strong physical security is a crucial foundation for effective cybersecurity. Lapses in physical security can lead to severe consequences, such as identity theft and data breaches. For example, an employee might leave a flash drive with sensitive information on a coffeehouse table, only to find it missing hours later. Similarly, old company bank records discarded in a rubbish bin could be retrieved by a criminal, or a burglar might steal files and computers from an office through an unlocked window.

To mitigate these risks, it is essential to implement stringent measures to protect both paper files and electronic devices. Here are some practical tips to enhance your physical security:

1. **Store Securely:**
   Ensure that paper files and electronic devices containing sensitive information are stored in locked cabinets or rooms. This simple step can significantly reduce the risk of unauthorised access.

2. **Limit Physical Access:**
   Restrict access to records and devices with sensitive data to only those employees who need it. By controlling who can access critical information, you can minimise the chances of accidental or malicious exposure.

3. **Send Reminders:**
   Regularly remind employees to secure paper files in locked cabinets, log out of networks and applications, and never leave files or devices with sensitive data unattended. Consistent reminders help reinforce good security practices.

4. **Keep Stock:**
   Maintain an inventory of all devices that collect sensitive customer information. Ensure these devices are secured and only keep files and data that are necessary. Knowing who has access to these devices and data is essential for accountability and security.

By integrating these physical security measures into your overall cybersecurity strategy, you can create a more secure environment for your organisation. Safeguarding your business against both physical and cyber threats is essential for building a resilient and secure future.

Ask Your Experts

Trusting the partners and vendors that you have in your supply chain is important. However, understanding how they implement their own cybersecurity measures to ensure that your organisation is protected is crucial. Below, we have outlined six key questions to ask your suppliers to ensure that your data is protected every step of the way.

Does your company adhere to any information security standards, or is there a formal security program in place? (e.g. NIST, ISO 270xx, CSA)

Do you have an individual or individuals in your company responsible for coordinating these information security measures?

Do you employ any controls to protect your organisation from any unauthorised or unwanted behaviour, such as antivirus, intrusion detection or network access controls?

Do you have a business continuity and/or disaster recovery plan in place? If so, how often is it tested?

Do you have internal policies that deal with how employees engage with information security measures and controls? Is there any formal or informal cyber security training or awareness provided?

Do you conduct, or submit any element of your infrastructure to penetration testing, either by internal staff members or by a third party?

Do you have a policy in place to measure the information security practices of third parties, such as cloud providers, suppliers and/or contractors?

PREPARATION IS KEY

What to do in the event of an attack

Report It

Engage your technology provider immediately. Report the scam to local law enforcement, the Garda National Cyber Crime Bureau, and the Data Protection Commission. You can also forward phishing emails to the Anti-Phishing Working Group at reportphishing@apwg.org, which includes ISPs, security vendors, financial institutions, and law enforcement agencies.

Notify Your Customer

Communicate with your customers promptly. Inform them of the breach, potential risks, and steps they should take to protect their information. Use clear, non-technical language and avoid hyperlinks in emails to prevent confusion with phishing scams.

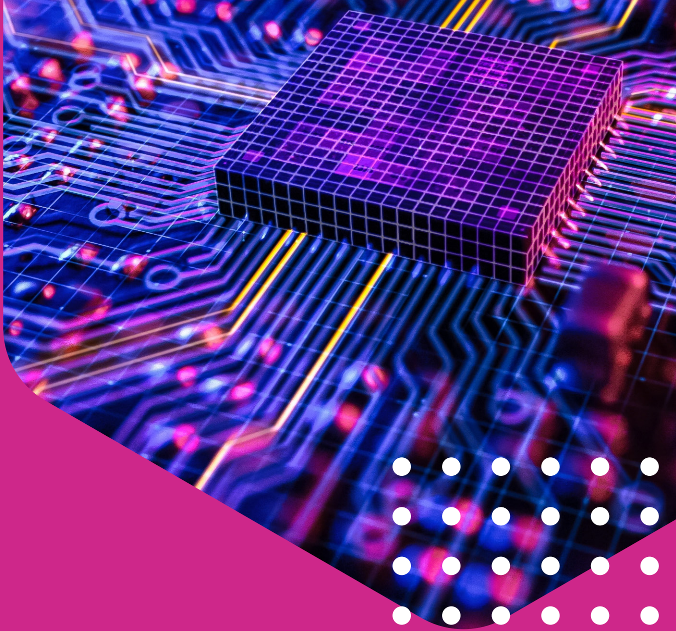
Alert Your Staff

Use this incident as an opportunity to update your security practices and train your staff about cyber threats. Ensure they are aware of the latest phishing and ransomware tactics and know how to respond to potential threats.

At Viatel Technology Group, we understand your business and your risk profiles. If you would like to learn more about our cybersecurity solutions, including network security, endpoint security, incident detection and response, employee security awareness training and ransomware containment, get in touch today by emailing

✉ hello@viatel.com

VIATEL
TECHNOLOGY GROUP



Discover more about Viatel's **Comprehensive Suite of Security Solutions** by emailing

✉ hello@viatel.com

🌐 www.viatel.com

AMTIVO ISO 27001 Certified Information Security Management

Microsoft Solutions Partner

Guaranteed Irish

PCI DSS certified Kyte Global

CISCO Partner

IRELAND BEST MANAGED COMPANIES Platinum Standard

Guaranteed Irish Business Awards 2024 Support Local, Look Global ptsb Winner Technology