CYBER SECURITY

FUTURE RANGE

Protecting Your Firm from Cyber Attacks

Cyber Security Advice for Accountancy & Advisory Firms

Reassuringly Excellent IT

Dublin | Limerick | Cork

futurerange.ie

Protecting Your Firm from Cyber Attacks

The escalating surge of cyber crime, underscored by the exponential growth of cyber attacks makes it one of the most pressing issues facing businesses worldwide, with professional services being high risk.

To safeguard your firm's reputation and avoid making headlines for all the wrong reasons, to do this necessitates staying current with the latest cyber security techniques and best practices. Understanding where to start to develop your firm's vigilance and implement robust security measures is key.

We will help you protect your firm from the potentially devastating consequences of a security breach, and also how to engage with your clients so they in turn can understand their vulnerabilities.

Our expert cyber security team can work with your firm to develop a strategic plan and manage risk.

Identify

Identify what assets (i.e. data and information) that need to be protected and determine the firm's current level of preparedness.

Protect

Protect the confidentiality, availability and integrity of the practice's core infrastructure to help ensure they're in regulatory compliance to avoid business-critical impacts.

Detect

Detect areas within systems and processes that are weak and vulnerable to assault by penetration tests and proprietary vulnerability scan tools.

Respond

Respond effectively to contain cyber-attacks and minimise the impact of the damage. To determine the entry point; what data was taken, and if there is any other suspicious malware still hiding.

10 steps to prevent a Cyber Attack

1. Educate Your Users
Provide regular cyber security awareness training to all employees.

2. Understand and Classify Your Data
Identify and classify the sensitive data your organisation possesses.

3. Embrace The Cloud
Leverage secure cloud services and platforms that offer robust security measures.

4. Carefully Manage Access & Identity
Ensure that only authorised personnel have appropriate access privileges.

5. Ensure Proper Password Management
Encourage the use of strong, unique passwords and enforce password policies.

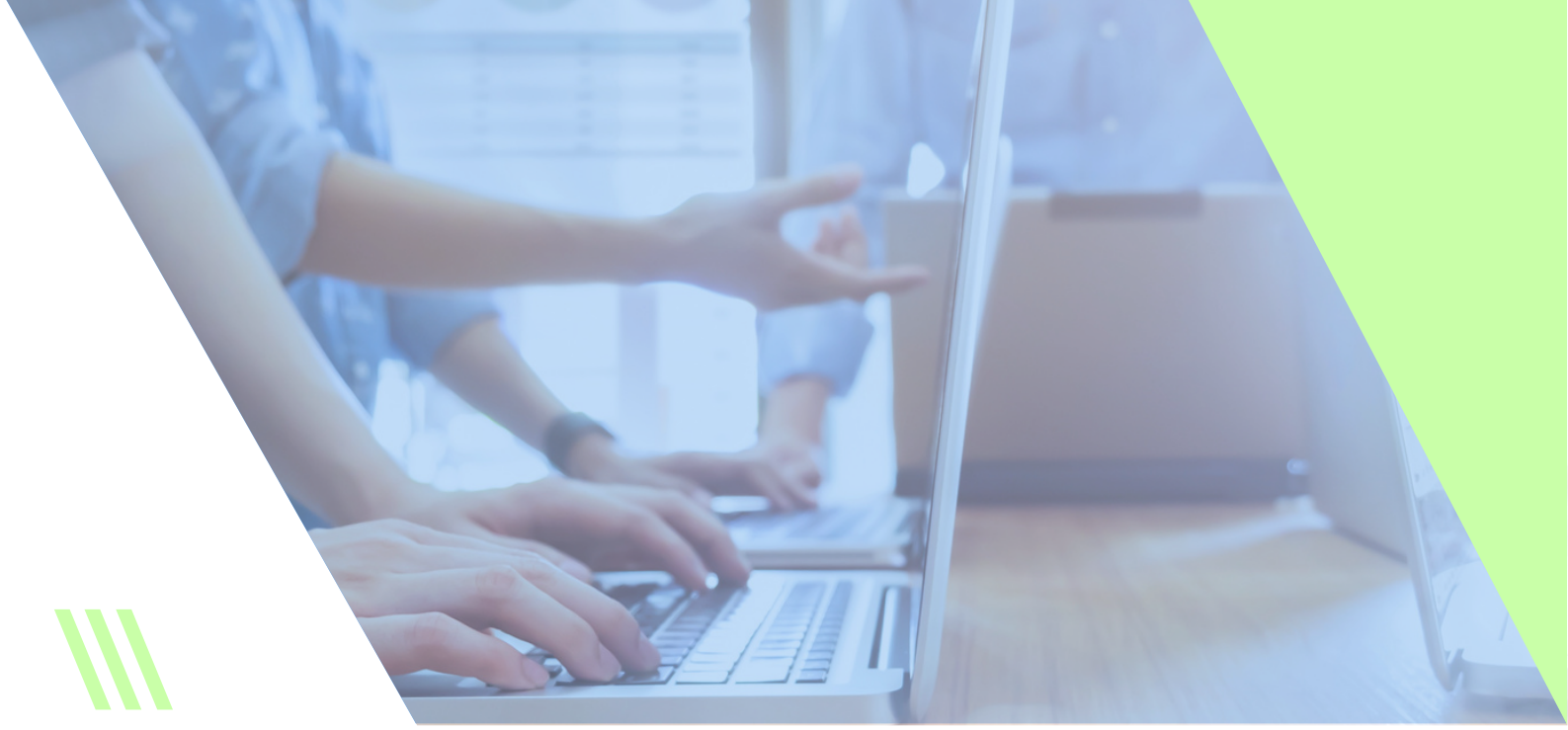
6. Set Up Multi-Factor Authentication (MFA)
Implement MFA wherever possible.

7. Encrypt Your Data
Utilise encryption technologies to protect sensitive data.

8. Backup! Backup! Backup!
Regularly back up your critical data and systems to secure offsite locations.

9. Ensure Your Software is Kept Up-To-Date
Regularly update and patch your operating systems, applications, and software to address known vulnerabilities.

10. Be Prepared
Develop an incident response plan to quickly and effectively respond to cyber-attacks.



What to do if your firm in is the victim of a Cyber Attack

Accountancy firms are a rich target for hackers because of the types of documents they handle. Beyond the normal personal identifiable information that they store for clients and employees, Accountancy Firms also handle sensitive information dealing with financial transactions, payroll information and sensitive business information.

Without a good cyber security strategy, these Accountancy Firms can suffer serious costs, including remediation of the security breach, reputation damage, and data privacy compliance penalties.

The steps you take after a breach can either increase or reduce the impact. Not having a cyber security response plan can lead to you paying much higher costs due to a delayed reaction.

IBM Security estimates that the global average cost for a data breach is €4.43 million. But organisations with a tested incident response plan can reduce that by €2.71 million, a savings of 39%.

Below sets out the vital steps that your Accountancy Firm should take immediately following the discovery of a data breach, ransomware incident, or another attack. Putting these into an incident response plan can save you millions in costs should your office suffer an attack.

7 Essential Steps if your Firm Suffered a Data Breach

1. Disconnect Infected Devices from Your Network

Many types of malware are designed to spread throughout a network as fast as possible. This is especially true for ransomware, which locks users out of their files through the use of encryption.

As soon as you discover that a breach has occurred, you should disconnect the infected device(s) from your network to try to contain the spread. This includes disconnecting the device from Wi-Fi and any hardwired ethernet connections and other systems including syncing cloud services.

You don't necessarily want to shut off the device's power until you have spoken to an IT professional.

2. Have a Professional Assess the Damage

Don't try to deal with a cyber breach yourself. Unfortunately, people can make things worse if they do things like try to go online to download some free virus scanning tool (that could actually be a malware trap).

Instead, once your machine has been isolated, contact a trusted IT Security Expert that can come and assess the damage and provide guidance. We have expertise and years of experience dealing with all types of data breaches and malware infections. This allows us to assess the issue and formulate a remediation strategy as fast as possible.

3. Remediate the Infection

Remediation of the infection is next. You don't want more of your client files being stolen while you're dealing with the fallout. Once the breach is assessed, your IT Security Expert will begin remediating the breach to secure your network.

4. Determine Whether Client Data Was Breached

Find out what type of data was compromised. Did the attacker gain access to a client database with names, addresses, phone numbers, client files or personal information.

This is not usually a pleasant task to determine the extent of the breach, all information held is sensitive so it's important to identify and notify impacted clients or third parties.

5. Contact Law Enforcement

Not every business will contact Garda National Cyber Crime Bureau (GNCCB) enforcement when hit with a data breach, even though they wouldn't think twice about doing so if this was a physical break-in. But data breaches are break-ins as well, so they should be reported.

Reporting the incident has a few benefits:

- You have a record of the incident for any potential insurance claims.
- ·Garda National Cyber Crime Bureau (GNCCB) can track the breach, which may connect to others that have been reported.
- Your report can be referred to in data privacy compliance reports and shows responsibility on the part of your organisation.

6. Carry Out a Notification Plan According to Data Privacy Requirements

You will need to review the data privacy regulations that your Accountancy Firm is subject to, such as GDPR, and make notifications to third parties according to their guidelines. If notification isn't made in a timely manner, it can lead to penalties, as well as a significant loss of trust in your business by those you need to contact.

7. Improve Defenses to Stop Future Breaches

Once, you've handled the most time-sensitive steps above, next, you will want to reinforce your defences to ensure this type of attack doesn't happen again. A good way to do this is by having a cyber security assessment performed.

A cyber security assessment can include penetration testing, which helps an IT Security Expert pinpoint specific weaknesses in your network that need to be fortified.

How we can help your firm

Our Experience

We have been at the heart of IT solutions in Ireland since 1995. Working in partnership with professional services firms of all sizes, we've carefully crafted a name that is now synonymous with trust, efficiency and value for money. Specialising in Cyber Security, our experts provide professional IT services for clients throughout Ireland and beyond, from our local offices in Dublin, Limerick, and Cork.

Our security team can develop and implement security measures and lay out a recovery plan for possible attacks. We can help you stay on top of cyber security trends and enable you to counter evolve cyber threats with complete confidence.

- Cyber Security Compliance
- Cyber Security Defense
- Endpoint Protection
- Managed Security
- Network Security
- Security as a Service
- Managed Security

Get in touch

Michael Rooney, Managing Director FutureRange

Michael is an accomplished professional with more than two decades of experience in the IT industry. As the leader of FutureRange, Michael is dedicated to helping clients access the best solutions for their firms.

His approach involves taking the time to understand the unique challenges, goals, and aspirations of each firm before developing tailored solutions that deliver tangible value, in protecting a firms most valuable assets.

Contact Michael today to schedule a consultation.

T 01 296 0560 | E mrooney@futurerange.ie