June 2025

The Mother Tongue

mother technologies

Cybersecurity Edition: One Click Away From Chaos

When the Wi-Fi Goes Down and the Shelves Go Empty. Cybersecurity Just Got Even More Personal

This Easter, disruptions were hard to miss. You went to grab your usual shop and the shelves were bare. Tried to order online? Error messages. Tried to pay at the till? Contactless not working. It wasn't panic buying. It wasn't poor planning. It was a wave of cyberattacks, and not just one.

In the span of weeks, M&S, The Co-op and Harrods were hit by serious cyber attacks. The fallout?

- Stock shortages and delivery delays
- Suspended online orders
- Click-and-collect systems offline
- Broken card machines
- Customer data compromised

What Happened at M&S Shows Just How Bad a Cyberattack Can Get

M&S was severely compromised by a major cyber incident. The impact it has had on the company is major:

- **£43 million per week** in estimated losses
- Online orders halted for over **6 weeks**
- Ongoing disruptions at physical stores
- Customer data (phone numbers, home addresses, DOBs) stolen
- Attackers demanded a ransom and sent abuse to M&S's CEO
- M&S finally resumed online orders, but their recovery is far from over.

Cyber experts confirm this was almost certainly a ransomware attack. This is where malicious software encrypts an organisation's systems, locking staff out of vital data and operations. The attackers then demand a ransom payment, often in cryptocurrency, in exchange for restoring access.

Co-op: Fast Action Avoided Catastrophe

Co-op was targeted by the same group, but its outcome was far less severe.

Hackers claimed they "spent a while seated in their network" and attempted to infect Co-op with ransomware. However, the Co-op's IT team acted early, pulling their systems offline as soon as possible, instead of trying to fight it like M&S.

While Co-op faced disrupted logistics, temporary shelf shortages, customer data breaches they avoided system-wide lockdown, ransom payments, or extended outages thanks to how fast they shut everything down. Whereas, M&S reportedly tried to fight the attack which ended up compromising them even further.

The attackers got into these businesses systems through a person, not a firewall.

- A phishing email.
- A moment of trust.
- A login handed over.

That was all it took. Cyberattacks don't break the door down anymore. They get invited in.

Nearly **88% of data breaches result from human error.**

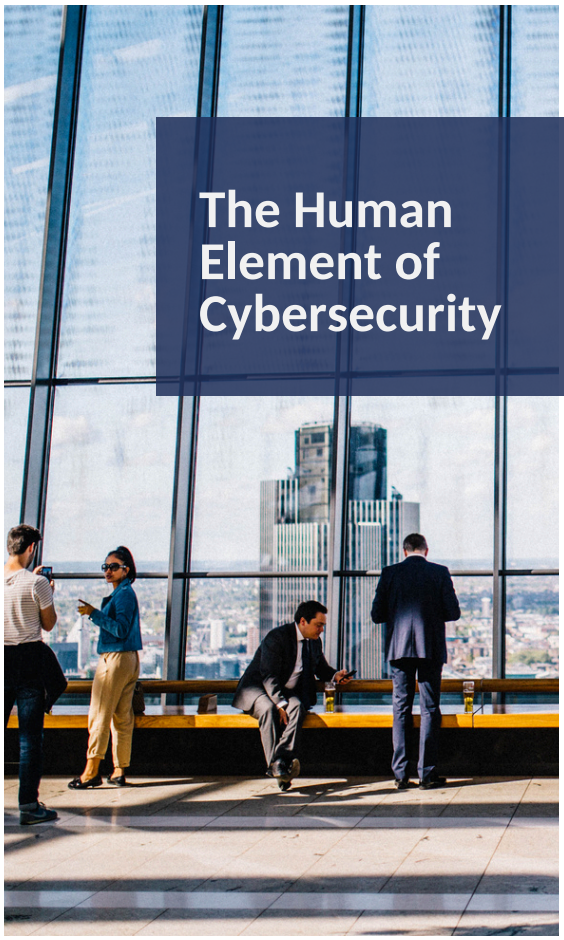
The cybercrime group responsible for these recent attacks, reportedly called DragonForce, operates like a SaaS platform for criminals, offering hacking-as-a-service.

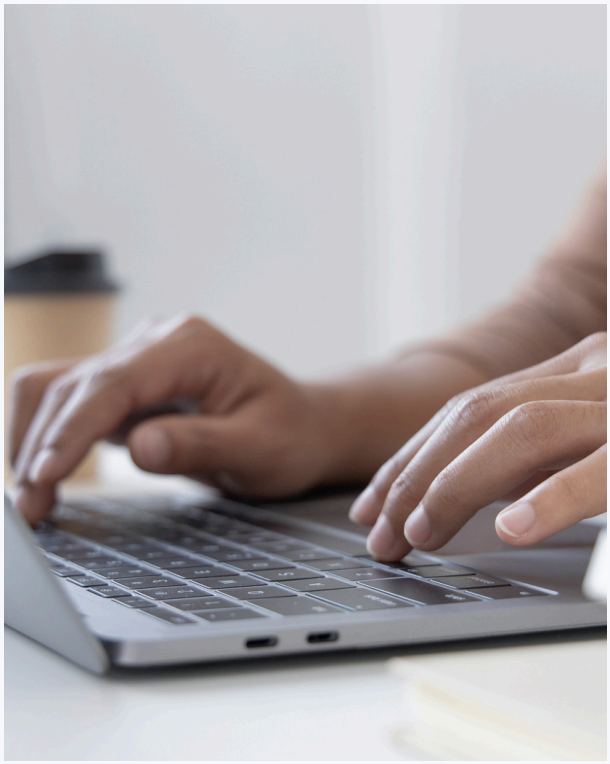
This includes ransomware tools and phishing kits.

They claimed responsibility for:

- The M&S attack
- The Co-op breach
- A failed attempt on Harrods
- Targeting other UK retailers

It is not about blaming people, but about **warning them and raising awareness.** These tactics the cyber criminals use work because they're so realistic, especially with the help of AI which allows them to create very convincing messages and exploit human trust more effectively than ever before.





"We are too small to be a target"

Small organisations should care more than ever. Why? Because cybercriminals know smaller organisations often lack strong security. Many still use outdated systems, rely on basic software, or operate on trust-based processes, the kind of gaps cyber criminals love to take advantage of.

If these large organisations with full cybersecurity teams can be breached, imagine how vulnerable your company is.

Cybercriminals don't care if you have 50 staff or 5,000, they care about your data, access to money, and connections to larger organisations. These attacks aren't just a minor disruption, they can be devastating.

The Risks are Real

The statistics show that **83% of small and mid-sized businesses aren't financially prepared to recover from a major cyber incident** *(Accenture 2024 Cybersecurity Survey)*, and **1 in 5 never recover after a ransomware attack** *(Datto Global State of the Channel Ransomware Report)*. Mother are here to make sure that your business doesn't become one of those statistics.

KnowBe4 – Cybersecurity Awareness Training That Works

KnowBe4 is the world's largest integrated platform for security awareness training and simulated phishing. **It helps organisations turn their biggest vulnerability, human error, into their strongest defence.**

What KnowBe4 Delivers:

- **Phishing Simulations:** Real-world phishing tests to help staff spot malicious emails before they click.
- **Engaging Training :** Videos, quizzes, and interactive content that doesn't feel like homework.
- **Risk Scoring:** Understand who in your team is most vulnerable and track their progress over time.
- **Automated Campaigns:** Set it up once and let KnowBe4 run ongoing training that adapts to your staff's needs.

KnowBe4, integrated with Mother's comprehensive RoundClock Security Suite, offers all round protection for your organisation. We help implement and manage your cybersecurity measures, increasing your resilience to cyber attacks.

Why Invest In Security Awareness Training?

"Most breaches start with phishing or weak human behaviour, not necessarily complex hacking. That's why basic cyber hygiene and awareness are so important in any organisation," says **Michael McLuckie, our Services Manager.**

"Security awareness training helps reduce the risk of cyberattacks, strengthens the human firewall element, helps meet compliance and regulation, protects company reputation and encourages a security-first culture.

It's far more cost-effective than dealing with a data breach or ransomware attack.

In short, security awareness training turns staff from potential liabilities into informed defenders, significantly improving a company's overall security posture."

KnowBe4

Action Plan: Immediate Steps if You Suspect a Cyberattack

Even with training, it's easy for someone to slip into autopilot. Clicking on a suspicious link, downloading an attachment without thinking, or responding to a convincing scam email. That's why having a clear, immediate action plan is essential.

IF YOU THINK YOUR PC MIGHT HAVE BEEN COMPROMISED

1.Shut Down your Computer Immediately

If your machine doesn't shut down normally, it may be that a malicious infection is preventing it from doing so. If that's the case, perform a hard shutdown by holding down the power button until the machine shuts down.

2.Report the Incident Internally

Speed is of the essence. Don't delay in reporting the incident to your manager or internal IT team.

3.Report the Incident to Mother

Unless your internal policies instruct otherwise, call us. Mother needs to speak with you directly to understand the incident in order to take appropriate action. Please do not use email, apps, or the Client Portal to report it. Phone us and explicitly declare your cyber threat concerns. Mother has an internal protocol to expedite potential cyber threats.

IF YOU THINK YOUR MOBILE DEVICE MIGHT HAVE BEEN COMPROMISED

Unless jailbroken, mobile devices, especially iPhones, are generally more secure than PC's. Nevertheless, your credentials may have been stolen and access to other services and your corporate network may be compromised. Take appropriate action.

1.Reboot the Device

Rebooting your phone or tablet interrupts running processes and flushes the memory.

2.Disable WiFi and Mobile Data on your Device

Once your device has rebooted, disabling WiFi and mobile data will prevent further Internet communications but you will still be able to make and receive calls.

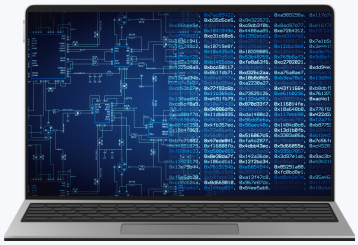
3.Report the Incident Internally

Speed is of the essence. Don't delay in reporting the incident to your manager or internal IT team.

4.Report the Incident to Mother

Unless your internal policies instruct otherwise, call us. Mother needs to speak with you directly to understand the incident in order to take appropriate action. Please do not use email, apps, or the Client Portal to report it. Phone us and explicitly declare your cyber threat concerns. Mother has an internal protocol to expedite potential cyber threats.

RANSOMWARE ATTACK



A ransomware attack might not always present as a pop-up message requesting funds or payment. Perhaps you're unable to login or access your device. Files may have disappeared or moved without explanation. Files may request a password or code to open them. Filenames may have been replaced with random characters or strange file extensions (e.g. .locked .xyz .encrypted).

1.Shut Down your Computer Immediately

If your machine doesn't shut down normally, it may be that a malicious infection is preventing it from doing so. If that's the case, perform a hard shutdown by holding down the power button until the machine shuts down.

2.Report the Incident Internally

Speed is of the essence. Don't delay in reporting the incident to your manager or internal IT team. Your internal IT team should:

- Pull the plug and disconnect your network from the internet
- Shutdown all systems

3.Report the Incident to Mother

Unless your internal policies instruct otherwise, call us. Mother needs to speak with you directly to understand the incident in order to take appropriate action. Please do not use email, apps, or the Client Portal to report it. Phone us and explicitly declare your cyber threat concerns. Mother has an internal protocol to expedite potential cyber threats.

What It Costs to Stay Secure

The cost of staying cyber safe is rising every year. Software, training, audits, and monitoring all add up and for many organisations, it can feel like a constant spend with no obvious return. It's understandable to wonder whether these investments are worth it, especially if you've never experienced a breach.

But this isn't a problem that's going away for any of us. It's only getting bigger and hoping not to be targeted isn't a strategy. It's a risk.

The reality is, cyber protections are no longer optional. Attacks are getting smarter and far more frequent. Whether it's ransomware halting your systems or a phishing email that catches someone out, the damage caused is rarely small and the recovery is always costly. It goes far beyond fixing systems: there are audits, downtime, lost revenue, reputational damage, a recovery bill that can quickly spiral.

We know these decisions aren't easy. But when it comes down to it, the choice is clear. You either budget for protection, or brace for the far greater cost of responding to an attack. Because while the investment in cybersecurity is real, the price of inaction is much higher.

Invest in protection or pay for recovery.

Key Takeaway: Speed is of the Essence

In cybersecurity incidents, speed is of the essence. Quick action can prevent widespread damage. If in doubt, shut down affected systems and contact Mother immediately.

Even well-trained individuals can make mistakes. What matters is how swiftly and effectively you respond.

At Mother our team knows your systems inside out, which means we're not only faster at detecting issues, we're faster at fixing them too.

When a threat strikes, there's no time to waste. We act immediately, using established protocols and clear communication to contain and resolve every incident.

Cyber resilience isn't just about prevention, it's about response. And that's where we stand out.

Partner Testimonial

"At Quorum Cyber, we regularly collaborate with a wide range of Managed Service Providers (MSPs) and during a recent engagement, we had the opportunity to work closely with Mother Technologies, an MSP offering IT, telecom, connectivity, and cyber security solutions to businesses in Scotland and beyond. Throughout the process, Mother's team demonstrated a high level of professionalism, clear communication, and a strong grasp of cyber security best practices.

Mother's deep understanding of their client environment, coupled with their responsiveness, ensured effective collaboration between all parties involved.

In an era where cyber threats are becoming increasingly sophisticated it's clear that Mother Technologies puts their customers' cyber protection at the forefront of everything they do. We look forward to opportunities to work together again in the future." - **Quorum Cyber, Edinburgh**