AI Cybersecurity Essential amid Harrods & M&S Cyberattacks. Steven Allan of Linten Technologies discusses why traditional antivirus precautions are no longer suitable when faced with the capabilities of modern hackers, and why AI-powered cybersecurity is.

Author: Steven Allan
Date: June 2025
From: Database and Network Journal(Vol. 55, Issue 3)
Publisher: A.P. Publications Ltd.
Document Type: Article
Length: 1,432 words
Content Level: (Level 5)
Lexile Measure: 1410L

Full Text:
Cybersecurity is like an old Cold War arms race, where new threats are followed by improved defenses--rinse and repeat.

According to the UK government's 2025 Cyber Security Breaches Survey, approximately 612,000 businesses (43 percent) and 61,000 charities (30 percent) reported cyber security breaches or attacks during the preceding year.

While an overall small decrease from 2024, this is mostly driven by fewer phishing attacks identified by small businesses. The report confirms that attacks aimed at medium to large businesses remain high.

So, it's imperative that they ensure their cybersecurity systems are fit for purpose.

New and emerging threats continue to plague businesses around the world, and following the recent damage inflicted on Harrods, Co-op and M&S, it's time companies realised that traditional antivirus (AV) deterrents may no longer be enough. Luckily, the future for cybersecurity is bright, with the emergence of AI- based tools that go far beyond current AV solutions.

Traditional antivirus shortfalls

Cyber threats tend to fall into one of two categories. The first are relatively unsophisticated, including phishing and impersonating organisations via emails or online, but many threats are increasingly sophisticated and capable of inflicting significant damage to logistics, technical infrastructure, and customer trust.

Traditional antivirus (AV) solutions rely primarily on identifying threats based on known virus signatures, but cybercriminals are becoming increasingly sophisticated, using advanced tactics such as social engineering and zeroday attacks to bypass traditional AV and firewall solutions.

One of the most famous examples of where AV was bypassed was the global WannaCry ransomware attack. In May 2017, the ransomware cryptoworm virus exploited a vulnerability in Windows, infecting over 300,000 computers internationally with damages ranging between the hundreds of millions and billions of dollars.

One victim was the NHS, which was particularly badly hit, with hospitals going offline and thousands of appointments and operations cancelled.

More recently, Harrods, M&S and the Co-op have fallen victim to successful cyberattacks, causing a myriad of challenges for staff and customers. M&S customers were unable to use contactless payment systems or use click and collect services, while the Co-op's call centre and backoffice systems were breached.

While most of these examples come from retail, cybersecurity threats aren't restricted to the sector. Charities, law firms, accounting

firms and government departments are all top targets for today's hackers.

According to a 2023 report from the National Cyber Security Centre, part of GCHQ, the UK's legal sector faces particular challenges as it routinely handles large sums of money and highly sensitive client information, which could be exploited in a number of ways.

What are the main types of threat?

Phishing attacks remain the most common, and most disruptive type of cyberattack, experienced by 85 percent of businesses and 86 percent of charities. Every day, billions of emails are sent daily by malicious actors, impersonating trusted senders. This adds up to over a trillion phishing emails yearly.

According to ESET research, the most common malicious attachment type is Windows executables (almost 50 percent), followed by script files, Microsoft 365 documents, and PDF documents.

With more people working from home, often connecting to unsecured networks, the risk of cyber incidents has increased drastically since the pandemic. Public Wi-Fi networks, commonly used by remote workers, are particularly susceptible to hacking, making them a significant concern for retailer, charities, law firms and even government departments.

Remote work also complicates the enforcement of cybersecurity policies and the monitoring of compliance. By preventing cybersecurity issues before they occur, organisations will greatly reduce the need for costly emergency fixes.

The cost of failure

There are many consequences from failing to prevent a cyberattack. The first is direct financial loss.

As we saw with M&S, cyberattacks can cause payment systems to be shut down, leading to a rapid spike in lost revenue. Such is the extent that M&S estimates the year's profits could be lower by around [pounds sterling]300m--an estimated third of its annual profit.

According to the government's report, only around 43 percent of businesses and 34 percent of charities are insured against cyber security risks. It can be reassuring knowing that funds are available to fix any damage caused by a successful attack, but the implications for businesses are far broader than their systems and immediate financial loss.

A metric that's very important for businesses but hard to measure is the integrity of its brand reputation. Whether the company is high-end like Harrods, or a convenience retailer like Co-op, customers must feel their data is secure and that they can shop with peace of mind. While it seems no customer data was breached during these attacks, many will have doubts about future purchases.

At the start of June this year, Cartier and North Face disclosed details of data breaches, with customers' names and email data stolen by criminals. These companies, alongside M&S, Harrods and Co-op, retain millions of pieces of data on customers around the globe. Ensuring they are stored safely must remain high in their priorities.

The third point of impact for businesses is how to fix a problem once identified. With press interest, concerned customers and lost income, reactively improving a cybersecurity system can be challenging, and if done hurriedly could cause future issues. A more streamlined approach using AI-based cybersecurity programs, however, is the best way to reduce future threats.

Al-based cybersecurity--the solution for the future

The nature and scale of cybersecurity threats is evolving rapidly and protecting IT systems and networks is a constant challenge. By investing in cutting edge AI-based cybersecurity programmes, companies stand a better chance of avoiding, or better responding to, the latest threats. Endpoint Detection and Response (EDR) goes beyond current AV solutions by providing continuous monitoring and analysis of endpoint activities. These systems collect data on endpoint events--including file changes, process executions, and network connections and use AI-powered behavioural analysis to detect suspicious or anomalous behaviour. If a ransomware attack is detected, EDR can immediately isolate the infected device, preventing the spread of viruses and minimising damage

Offering real-time monitoring and analysis, proactive EDR helps to mitigate cybersecurity threats that would otherwise go undetected by traditional, reactive AV alternatives.

When a threat is detected, EDR will automatically isolate the affected endpoint, terminate malicious processes, and alert security teams. In real terms, this gives companies more time to act and with better insight into what the threat is.

Adding Managed Detection and Response for a full cybersecurity solution

On top of EDR systems, companies can benefit from greater protection with a Managed Detection and Response (MDR) solution.

EDR and MDR combined provide more advanced and proactive approaches to dealing with a broader range of cybersecurity challenges, incorporating behavioural analysis and human intervention to enhance detection and response capabilities. MDR is also ideal for businesses and charities with stringent compliance requirements as it automatically generates reports showing threat detection, investigation, and response activities.

When combined with advanced AI technology, MDR identifies and deals with risks associated with privilege abuse, account takeovers, and insider threats, safeguarding critical business systems and reducing the overall capabilities of a cyber security threat.

The importance of training staff

According to a study by IBM, human error is--incredibly the main cause of 95% of cybersecurity breaches.

All levels of an organisation must be engaged and educated about cybersecurity best practices. This includes recognising phishing attempts, understanding the risks of unsecured networks, and following robust data protection protocols. Educated employees remain the first line of defence.

These are some of the most relevant and useful certifications for key members of staff:

* ISO/IEC 27001 for Information Security Management.

* Cyber Essentials & Cyber Essentials Plus

* Certified Information Systems Security Professional (CISSP)

Government bodies including the National Cyber Security Centre (NCSC) and legal institutions like the Law Society also provide resources for best practice and guidance to help firms enhance their cybersecurity capabilities.

A checklist for businesses to avoid becoming the next headline

1. Analysis whether current cyber security infrastructure is fit for purpose in today's digital environment

2. Learn more about how threats are evolving and the expectation of future weak points

3. Invest in a system that's designed for modern threats, and futureproof against threats of the future

4. Ensure staff undergo regular training, especially if they work remotely.

Charities and companies in all sectors must be aware that new threat types are appearing with increasing regularity, and that advanced solutions that go beyond checking virus signatures are now essential if they are to stay fully protected. It's time to bid farewell to AV and embrace a new age of proven security with EDR and MDR.

www.linten.co.uk*

Please Note: Illustration(s) are not available due to copyright restrictions.

Source Citation (MLA 9th Edition)
Allan, Steven. "AI Cybersecurity Essential amid Harrods & M&S Cyberattacks. Steven Allan of Linten Technologies discusses why traditional antivirus precautions are no longer suitable when faced with the capabilities of modern hackers, and why AI-powered cybersecurity is." *Database and Network Journal*, vol. 55, no. 3, June 2025, pp. 17+. *Gale In Context: Science*, link.gale.com/apps/doc/A847780220/SCIC?u=king56371&sid=summon&xid=90b5656b. Accessed 29 Sept. 2025.
Gale Document Number: GALE|A847780220