HANDD
BUSINESS SOLUTIONS

CYBERSECURITY BREACH REVIEW 2024:

THREE TALES OF ORGANISATIONS GETTING IT WRONG

What do Dow Jones, Tesla, and an established healthcare provider have in common? They all got into the news for the wrong reasons. Their cybersecurity was tested and found wanting.

CYBERSECURITY INCIDENTS UP 52% IN FINANCIAL SERVICES [1]

A report that we shared in 2018, *Year of the Defender*, made, among others, a reasonable core prediction: breaches would continue, and the global destructive effects of poor cybersecurity would cost businesses dearly. To the surprise of very few, it all came true.

The UK Government's latest Cyber Security Breaches Survey reveals that cyber attacks have evolved and become much more frequent. Around a third of businesses report suffering at least one cybersecurity breach or attack in the last 12 months, and around one in four was a highly sophisticated attack type such as spyware, malware, ransomware, or denial of service. [2]

In our latest report, we highlight three of the most notable data breaches in recent times, looking at what happened, how it happened, and what could have been done to stop hackers in their tracks.

Fair warning: These aren't pretty.

1 Source: UK Financial Conduct Authority (FCA) 2021
2 Source: Cyber Security Breaches Surveys 2023. Gov.UK.

DOW JONES: WIDE-OPEN, UNPREPARED AND UNAWARE

CLOUD EXPOSED

If you thought historic global organisations were exempt from business-critical data leaks, you'd be wrong.

Dow Jones & Co, a stock index active since 1896, suffered a humbling PR nightmare in 2019 when a simple but far-reaching mistake was uncovered: the names and contact information of 2.2 million customers, former politicians and 'high-risk individuals' - all accesible with no password on a public cloud storage server. Every entry was indexed, tagged and searchable.

DOW JONES' PROBLEM

The cloud contains many freely available tools to share information; the technology in this particular breach is just one of them. Users aren't necessarily on the lookout to breach security controls but they need to share files to do their jobs and will, in most cases, use whatever they're comfortable with.

WHAT WENT WRONG?

LACK OF AWARENESS

Dow Jones' IT decision-makers perhaps didn't understand or, it seems, appreciate vital cloud access control mechanisms. Leaving this much data – including email and home addresses and partial credit card information - publicly available on the cloud is an exceptionally basic security oversight.

POOR FILE TRANSFER METHODS

Moving data to the cloud isn't a 'fire and forget' action; real attention must be given to the new security considerations it brings. Cloud storage is an entirely different format, deserving at minimum a project rigorously assessed by IT security experts.

WHAT COULD HAVE HELPED?

Standardised file transfer processes: We can only speculate on what led such a respected company to make such a basic mistake, but incidents like these commonly occur due to poor processes.

In this case, there was lack of visibility and no clear process for the transfer of sensitive data. As a result, Dow Jones staff erroneously moved data from local storage to an insecure cloud location. MFT would have been a safer alternative to popular cloud file transfer solutions, flagging security issues like this immediately.

Managed file transfer: In a similar vein, managed file transfer would have given Dow Jones & Co the easy security they lacked at the time. Simply put, MFT servers give companies and their users a compliant data store alternative; modern MFT servers include audit trails and customisable levels of security and empower users to share information without losing it in the cloud to insecure or less trusted platforms.

Remember, this was a very basic mistake for Dow Jones & Co to make, and it's exactly the kind of leak an investment in an MFT server or service would avoid entirely. Fortunately for Dow Jones & Co, this occurred pre-GPDR; if it had happened after the new legislation came into effect, the fines could have been in the region of hundreds of millions of Dollars.

LESSONS LEARNED

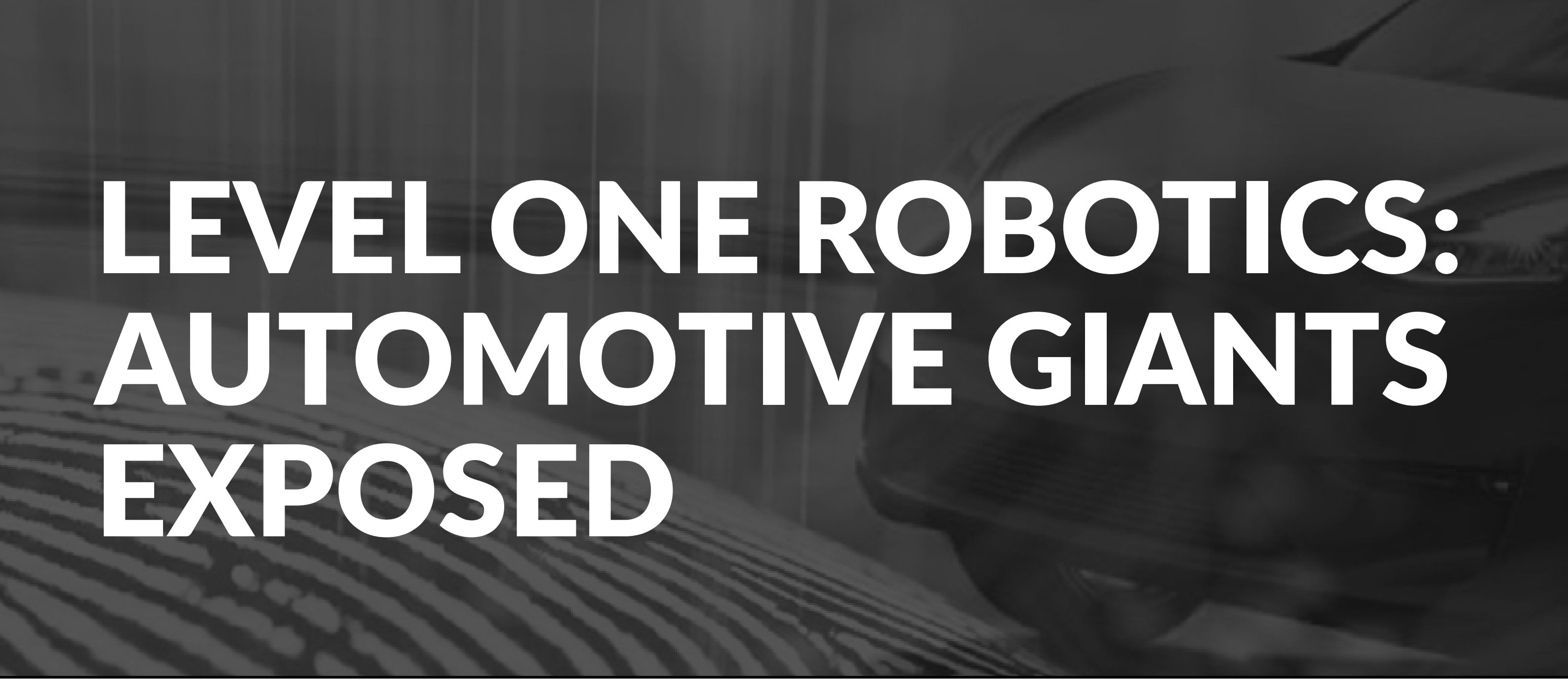
An eventful few years, and an obvious trend: it isn't always about sophisticated attacks breaching advanced systems. We're talking serious companies with gaping cybersecurity issues that could easily have been resolved.

As business leaders, it's easy to write off cybersecurity as an unreasonable investment, requiring the most powerful of systems and policies to be effective.

The truth? It's more about the basics. About knowing what data you have. Knowing how it's accessed. Having simple, but consistent training and evaluation in place.

A modest investment, then, that could have stopped these three companies from being in the news for all the wrong reasons.

As value propositions go, that's hard to beat.



LEVEL ONE ROBOTICS: AUTOMOTIVE GIANTS EXPOSED

OPEN TO THE PUBLIC

Tesla. General Motors. Ford and Toyota. All compromised.

Thanks to the diligent efforts of a cybersecurity research company, these titans of the automotive industry – and 100 more companies with them – were in July 2018 found to have had sensitive documents stored on a publicly accessible server.

In this case, the server was owned and operated by industrial automation service provider Level One Robotics – a supplier of all the aforementioned companies.

In addition to detailed vehicle schematics and NDA-bound invoices, contracts and bank account details were found alongside scans of driving licences and staff passports.

WHAT WENT WRONG?

Budget: In this instance, budget may have been an influencing factor in the breach. Level One Robotics made regular use of an unrestricted rsync server. Rysnc is a free utility tool used for the transfer, sync and backup of files across systems and servers.

Unfortunately for Level One Robotics – and many the organisations they supply – this unrestricted access allowed any rsync client able to connect to the server's port and download every file within. It is unclear if, or to what extent, this was done by any other party that may have uncovered the vulnerability.

Data discovery: Level One Robotics was unaware of the extent of data stored in such a location, particularly in regard to NDA documents and copies of staff ID. Data discovery often involves performing data audits with the end goal of knowing exactly what data is owned and where it is stored.

Such a clear cybersecurity issue may have been flagged and resolved if this activity had been considered and performed.

AN INTRO TO MFT

Managed file transfer (MFT) is a technology platform that manages the secure transfer of data from one location to another, both internally and externally through a network, all from one centrally managed interface. MFT provides an enhanced level of control and visibility over the movement of data, improving an organisation's operational efficiency and supporting regulatory compliance requirements.

This report details the stories of three data breaches that could have been prevented if a properly configured MFT solution was used to move data and files.

Whether it is proprietary data, employee or patient information, credit card data or insurance documents, MFT provides the ability to exchange files and data securely, quickly and reliably.

WHAT COULD HAVE HELPED?

Prioritising cybersecurity: As stated by Automotive Information Sharing and Analysis Centre executive director Faye Francy, most car makers' usual 'top cybersecurity priority is vehicle risks'. Corporate documents on an unsecured server – particularly in this instance – may fall behind in investment by comparison.

With data laws relating to cybersecurity tightening by the year, this is a dangerous mindset. New fines, such as the percentage of annual turnover possible under GDPR, go hand in hand with PR damage to devastate businesses and corporations all over the world.

Investment in secure file transfer and storage: A key draw of the rsync tool is its price: it's free. While effective in its ability to transfer and synchronise files, it lacks robust security functionality that is needed to protect a business from increasingly costly breaches – a problem that is doubly relevant with GDPR in effect across the UK and Europe.

Robust cybersecurity, including the use of solutions such as Managed File Transfer, is rapidly becoming mandatory for any business that wishes to avoid being in the headlines for the wrong reasons.

A configured MFT application: The implementation of an MFT application over the free rsync solution could have saved Level One a serious amount of trouble. We've identified three key ways in which it could've helped:

1. **Gateway:** A software specific gateway can prevent direct access to a network hosting sensitive data. Data can be exchanged over encrypted tunnels, and authorisation, authentication and accounting are handled separate to the data itself.

2. **Auditing:** Generally speaking, freeware doesn't provide the best auditing and reporting, and rsync is no exception. Although verbose flags can flood log files with data, it's often unfiltered and of lower relevancy, still requiring manual review. A solid MFT solution is more concise while still reporting key metrics like logins, downloads, uploads, and timestamps for such activity.

3. **Configuration:** Any daemon running at operating system level should be treated with care. Default configs are often unsecure, with changes needed to things like access control lists to ensure users can't simply move around the full directory tree. MFT systems are the opposite by default, being underexposed by design, only allowing exposure of business-critical data to appropriate users.

MEDEVOLVE: UNSECURED AND EXPOSED IN THE HEALTHCARE SECTOR

NOT SO GLAMOROUS

Hollywood often portrays the process of hacking as glamorous. Rooms are filled with screens of sprawling code and only the brightest minds can penetrate sophisticated defences.

USA-based medical software company MedEvolve's breach was, perhaps, humbler in that regard when in 2018 an FTP server was found to permit anonymous login and did not require login credentials, exposing a database of 205,000 records of sensitive patient information, including names, addresses, and 11,000 social security numbers.

MFT OVER FTP

Every business needs to transfer files and data. Failure to proactively monitor the journey of that data can result in missed SLAs, poor compliance procedures or even business-critical data breaches. MFT overcomes these risks by offering improved data transfer security, control and visibility from one centrally managed interface.

WHAT WENT WRONG?

NO PERMISSION AND ACCESS CONTROLS

No process was in place to maintain and monitor access. By checking networks and default permissions and credentials regularly, MedEvolve could have identified the threat earlier.

INADEQUATE SECURITY AWARENESS

Informing employees of basic cybersecurity principles could have avoided such heavy use of the unsecured server, as well as providing the opportunity to identify the threat before it got worse.

NO SYSTEM CONFIG MANAGEMENT

Processes concerning password use and file auditing and permissions could, at least, have partially protected the server files. Without these, the door was left open for hackers.

NO DATA CLASSIFICATION

A policy of classifying data – where files are required to be categorised individually based on their sensitivity and importance – could also have aided MedEvolve here.

WHAT COULD HAVE HELPED?

Staff training: Basic training on the principles of cybersecurity and secure file storage may have avoided this costly affair entirely. Without this, staff continued to use the server, instead of being trained to identify it as a potential threat or issue.

Managed File Transfer: An MFT server would have given MedEvolve the data security they sorely needed. MFT servers allow staff to securely transfer files internally, externally and on an ad-hoc basis.

The server authentication and data encryption methods common to MFT would also have given MedEvolve a valuable audit trail, potentially helping to identify individuals who may be demonstrating poor cyber and data security awareness.

As we noted in regards to a recent Equifax breach, the configuration of a solid MFT system would not only increase security, but make tailoring it easier – a single click to disable anonymous logins across all services, for example.

Moving from a free or homegrown system to such a solution ensures basic flaws like this are eliminated by default, as well as providing user and password management abilities for relevant services – without altering the operating system itself.

USE CASE - FIDELITY INTERNATIONAL

Fidelity International approached HANDD to help source and implement a MFT solution. After a thorough market analysis, HANDD implemented a MFT product integrating with Fidelity's other applications to streamline workflow. In no time the product was delivering more secure file transfers.

HANDD
BUSINESS SOLUTIONS

HANDD Business Solutions (HANDD) advises clients on keeping their data safe - at creation, at rest, in use and in transit. Delivering truly agnostic advice on data security, HANDD removes traditional barriers for the adoption of new or alternative data security, giving each organisation the freedom to choose data security solutions to suit their specific business needs.

HANDD has become a trusted partner to more than 700 customers in 27 countries around the world, delivering independent advice on the identification, integration and roll out of data protection platforms. By delivering training and support through deployment and beyond, HANDD ensures customers continue to get the best return on their investment throughout the entirety of its lifecycle. HANDD works with a range of market-leading vendors and brings a wealth of experience to complex integrations for faster, smoother and easier platform deployment to protect the asset that resides at the heart of every modern business – data.

www.handd.co.uk
info@handd.co.uk
+44 (0)8456 434 063