CASE STUDY

Global Pharma, Global Target, Global Response

TRANSFORMING A WORLD-RENOWNED COMPANY TO WITHSTAND CYBER-ATTACK

Medicare Network

More intelligent, More Secure

COMPANY PROFILE

Medicare Network is a niche, forward-thinking cybersecurity and risk management company dedicated to solving the healthcare and pharmaceutical industry's most important cybersecurity challenges. Providing proven experience, expertise and individuals who share the passion in preventing the most sophisticated and targeted cyber-attacks to critical infrastructure and life-critical medical technologies.

We are a vendor agnostic company that carefully identify and select world-class innovative cybersecurity solutions that leverage the latest cloud, with Artificial Intelligence (AI) and Machine Learning (ML) powered capabilities. To intelligently detect and respond to any potential cyber threats to IT, and Operational Technology (OT) systems and infrastructures.

Delivering security transformation and driving better value in the age of digitalisation!

AT A GLANCE

- Pharmaceutical multinational deemed 'not fit for purpose' to withstand a cyber-attack
- Huge exposure to nation-state sponsored hackers, threatening years of investment and research
- Disparate security systems and unmanageable data impaired threat visibility, and response
- Variable security maturity levels; solutions combining automated security testing, compliance and risk management controls, processes, reviews, initiatives, and training
- Strengthened visibility of, and resilience to, cyber threats; alignment with globally recognised information security standards and guidelines (ISO27001, ISA/IEC 62443, NIST CSF, NIST 800-53 and NIST 800-82) and mandated directives (GDPR, NIS, HITECH and HIPAA)
- Increased digitisation and secure online data storage; delivering massive cost savings estimated at hundreds of millions of dollars over the next 3-5 years

THE CLIENT

A multinational pharmaceutical company with a worldwide presence, this client is one of the largest and most respected pharma industry players. Its research and development and manufacturing operations span the globe and has several joint ventures with other major pharmaceutical companies.

BACKGROUND

The pharmaceutical industry remains a prime target for nation-state sponsored hackers and ever-evolving cyber threats. An industry built on innovation, with extensive investments in Research and Development (R&D), Intellectual Property (IP) relating to drugs and medicines, pharmaceutical advances and technologies. Patient health data from trials spans the disciplines of the organisation creating increased network complexity, and making it a 'hot spot' in the health data threat landscape.

Data created, collected, stored and processed is highly sensitive, which means that losing control over that data can have catastrophic consequences. Additionally, the industry holds strict privacy guidelines regarding the safeguarding of Protected Health Information (PHI), which highlights the need for an effective cybersecurity strategy.

An independent external audit of the organisation discovered how cybersecurity defences were 'not fit for purpose' to withstand a cyber-attack. In parallel, the entire industry had also become subject to a Presidential Executive Order in the United States, mandating an increase in the level of core capabilities for critical and essential infrastructure to protect against, and manage cyber risks.

Consequently, a new information security programme was deemed critical to maintaining the credibility, and reputation, of the organisation, focusing initially on ISO27001 compliance. Rapidly became apparent that traditional security and compliance efforts were not in step with the more comprehensive security demands driven by digitalisation, transformation and risk appetite of the US Government mandate.

Medicare Network engaged closely with the client, advising that a more 'holistic' approach would deliver far greater benefits, not only establishing a more comprehensive and responsive cybersecurity operation built around standardisation, consolidation, and shared services, but also delivering significant business transformation by these same means.

In short, Medicare Network identified a significant opportunity to make the organisation more secure and operationally efficient. This was achieved by adopting NIST Cybersecurity Framework (CSF) to identify, reuse and adapt existing processes, aligned to ISO27001, and ISA/IEC 62443.

THE CHALLENGES

From a cybersecurity perspective, the client's challenges were extensive, and deeply ingrained in the company's IT culture, and data organisation. For years, the company had 'bolted on' security with 'point' products to address specific security or compliance requirements separately and narrowly, leaving the organisation with:

UNMANAGEABLE DATA, UNIDENTIFIED THREATS

Huge volumes of historical and largely unstructured or poorly structured data, essentially made it impossible for the IT team to drill down into the detail, in order to find and react to genuine or less obvious threats that could have significant business impact. This in turn, meant the team was focused only on signs of easily recognisable attacks, which tend to generate many false positives – each one a costly waste of valuable security resources.

DISTRIBUTED SYSTEMS, FRAGMENTED RESPONSES

The client operated a decentralised, non-SIEM environment, meaning their end-to-end visibility was lacking, security events and alerts are not detected or understood. Lack of communication between products, threat response cannot be automated and is not fast or effective. This is a highly ineffective and inefficient means of determining the root cause of an event or incident, as well as how to respond. Time to remediation was therefore dramatically increased, potentially risking far greater financial loss, operational impact, and reputational damage.

SHADOW IT: INVISIBLE, THEREFORE UNDEFENDABLE

A lack of visibility creating several high-level problems beyond just the security gaps were inherent in this approach. Weak and unenforced IT policies had led to extensive 'shadow IT' assets – cloud-based services, developments, data, devices, and endpoints - that had been adopted unofficially outside the IT and security operations estate, with potential vulnerabilities, or indeed very existence, were often, therefore, invisible.

DATA EXPOSURE AND INEFFICIENCIES

Highly sensitive data was often stored in shared and insecure repositories; the lack of central encryption management and keys made the process of attempting to secure the repositories administratively burdensome and highly inefficient - the result being that it often remained unencrypted and therefore highly vulnerable.

SECURITY AS AN AFTERTHOUGHT

With no formal process to ensure that information security was a non-negotiable sign-off requirement for every IT development project, every such new development – including those designed to deliver business transformation – and the introduction of other digital innovations also contributed to the potential increase in the attack surface of an already expanding and complex network. This included cloud migrations, connected medicine and telehealth, the proliferation of endpoints, and the surge in remote working.

IOT AND IIOT: UNIDENTIFIED, INSECURE AND UNMANAGED

As digital innovation and business intelligence gains compelled Operational Technology (OT) networks to converge with IT networks, OT devices and systems were not created with security in mind and were dependent on an air gap for separation. Poor visibility of internet-enabled and connected devices - Internet of Things (IoT), and Industrial Internet of Things (IIoT) device integration via OT/IT convergence - offered cyber criminals the opportunity to exploit inherited vulnerabilities.

THREATS FROM WITHIN

The audit identified a lack of controls and procedures for insider threats. Damage from insider sources can be hard to detect because these threats encompass a wide range of behaviours and motives. It could be a disgruntled employee attempting to disrupt operations, a staff member looking for financial gain by selling trade secrets, or a well-intentioned co-worker who merely sidesteps company policy to save time.

COMPLIANCE CONCERNS

As regulatory requirements evolve and become more complex, the difficulty of manually achieving enterprise-wide visibility and enforcing the required security controls only increases. But the organisation's enterprise was composed of disparate point products that did not share reporting capabilities, rendering compliance efforts both ineffective and time-consuming.

PEOPLE-AND-PROCESS GAPS

With both global and regional lines of business, and a vast user population, there were no robust or interconnected structures in place to enable information security issues to be regularly debated, buy-in, budget, and actions to be agreed, cybersecurity training to be delivered, or appropriate governance, risk and compliance oversight put in place.

> “BY THE GROUP CIO’S OWN ADMISSION, ‘WE FAILED SEVERAL SECURITY AUDITS, AND IT JUST SEEMED THAT EVERY TIME WE DID SOMETHING TO IMPROVE OUR BUSINESS, WE ALSO DID SOMETHING TO COMPOUND OUR CYBER RISK. WE THOUGHT GAINING ISO27001 CERTIFICATION WOULD SOLVE THE ISSUE. HOWEVER, MEDICARE NETWORK’S INSIGHT CONVINCED US THAT A MUCH BROADER APPROACH WAS NEEDED, BUT THAT THIS WOULD ALSO DELIVER SIGNIFICANT DIGITAL TRANSFORMATION UPSIDE AND COST SAVINGS.”

THE SOLUTION

It was important to understand exactly what the current security and compliance failings were, and what their likely consequences could be. To this end, Medicare Network reviewed existing audits, compliance and risk assessment reports going back three years, addressing critical issues across people, process, technology and physical environments.

Rather than try to solve each issue separately, a tactical and strategic plan was devised to take a more comprehensive, architectural approach to addressing cybersecurity and governance.

From this, Medicare Network developed a comprehensive security strategy focused around seven key objectives:

1. **Integrating security ‘point’ solutions that are woven into the network infrastructure,** enabling the organisation to be agile with organisational growth and digital transformation. Such an approach provides the automation, visibility, and fast response to threats that easily demonstrate compliance and defend against cyber-attacks enterprise wide.

2. **Securing and accelerating business application development** via containerisation, using tactical and strategic technical and process controls.

3. **Reducing third-party cyber risk** by developing a supply chain risk management accreditation programme for all suppliers and partners.

4. **Combining security transformation and digital transformation,** to exploit approaches beneficial to both (e.g. transitioning infrastructure, applications, management information and historical data to the cloud; implementing secure digital workplace SaaS-based solutions, AWS, Microsoft Azure and 365).

5. **Facilitating dialogue and joined-up thinking,** by the creation of Global and Regional Cybersecurity Business Forums, to agree cross-organisational objectives, initiatives, priorities, and accompanying security budgets and actions.

6 **Making security the primary authority** on IT and data decisions, through the creation of a Governance, Risk and Compliance Steering Committee, and a Design and Architecture Review Board, to oversee all IT, OT, information security, cybersecurity, and projects.

7 **Protecting against 'unknown' threats,** by deploying innovative AI/ML solutions that can interpret suspicious network activity and behaviours, thus identifying emerging and sophisticated threats that are not known in any threat or intelligence databases.

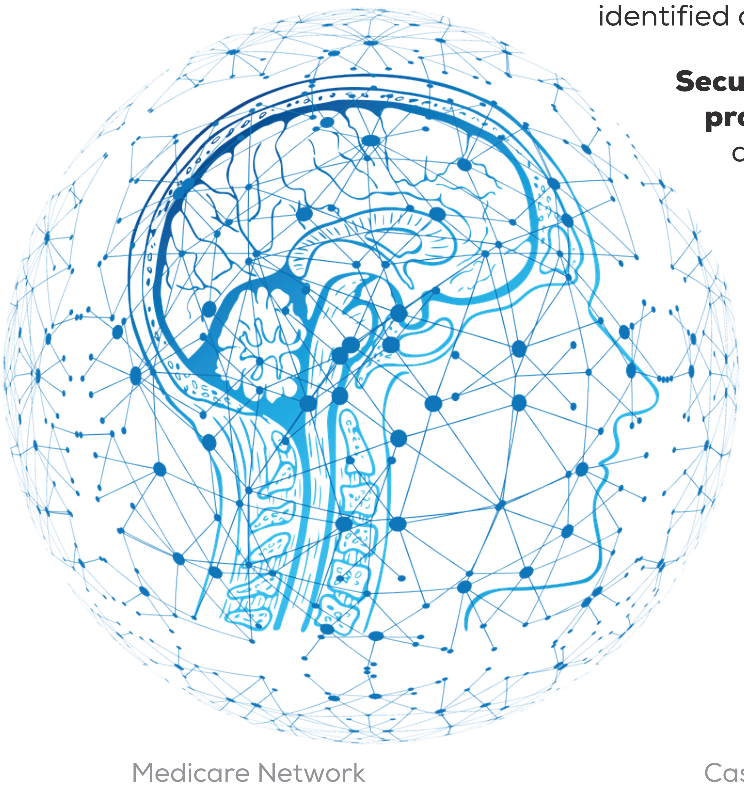
Specific initiatives within these objectives including the introduction of Business Impact Analysis (BIA), new and comprehensive group cybersecurity policies and standards, the introduction of enterprise-wide encryption, security awareness and compliance training, and the transition to secure communications and collaboration tools for data exchange and secure transfer methods.

OUTCOMES AND RESULTS

Strategically, the programme Medicare Network delivered enabled the client to achieve far wider business-critical information security compliance than the ISO27001 certification itself would have conferred.

Data was classified and stored according to its relative risk and criticality, to ensure handling and management was secure both in transit and at rest, delivering a far more transparent security environment.

Automated testing processes were integrated to perform continuous security assurance testing of network infrastructure and applications, which was also embedded into the software development life cycle to ensure that potential risks, flaws and vulnerabilities were identified and addressed.



Security was 'baked into' infrastructure projects, application development, supplier and partner relationships, and sign-off processes across the organisation, ensuring the business's evolution did not simultaneously become its undoing.

Unifying systems and transitioning to cloud created not only a more agile and flexible business environment but made it possible for security to be centralised – including IoT, IIoT, and industrial process systems – and shadow IT connections to be discovered, delivering monitoring, detection, and response from a 'single pane of glass'.

Consistent security access controls were deployed to mitigate insider threats, and security measures implemented to examine network traffic and determine the appropriate course of action. Identity and privileged access management practices were implemented to help limit insider threat paths, and provide robust end-to-end audit trails.

Backup and recovery were instigated regularly and segregated from the production environment. In the event of an operational impact, (e.g. ransomware attack) data was then easily recoverable from the backup environment.

A security culture was created where employees understood cyber threats and good practices they needed to follow to protect confidential information and critical systems. A security awareness program encouraged and enabled employees to play an active role in the company's overall security strategy.

And the **dialogues, forums, training, and other human initiatives** put in place enabled cybersecurity to take a place at the 'top table' of the business's internal conversations.

From failed audits and regulator sanctions to wide-ranging compliance and a transformative, cloud-based operating model – this is just another example of how Medicare Network delivers above and beyond.

PASSIONATE PEOPLE, DEDICATED TO YOUR SUCCESS!

The changing landscape and constant evolution of cyber threats means that protection-levels and education for staff is a continuing process for every business.

Medicare Network's primary focus is providing integrated security transformation services and solutions to healthcare providers and pharmaceutical organisations of all sizes to prevent, detect and, recover from a security incident or breach.

FOR MORE INFORMATION

- UK/EMEA +44 (203) 355-3785 - US +1 (702) 605-4601 - clientservices@mednetsec.com
- Mortlake Business Centre | 20 Mortlake High Street | London | SW14 8JN | United Kingdom
- www.mednetsec.com

© 2021 Medicare Network, Limited. All Rights Reserved.