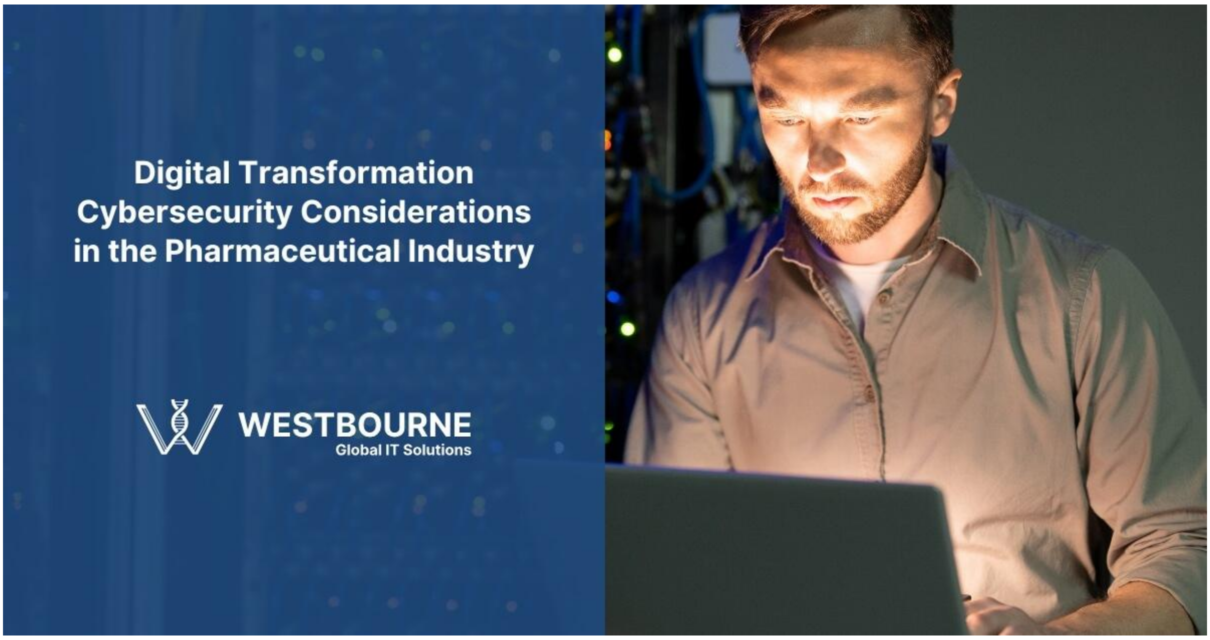
Digital Transformation Cybersecurity Considerations in the Pharmaceutical Industry


Digital Transformation Cybersecurity Considerations in the Pharmaceutical Industry
WESTBOURNE
Global IT Solutions

Companies in the pharmaceutical industry cannot stand still, so modernising through digital transformation is essential. It is also a fact that companies in the pharmaceutical industry are high-value targets for malicious actors and cybercriminals. This cybersecurity threat risk applies to companies in their present state, let alone when digital transformation initiatives lead to technology and operational changes.

Digital transformation is a necessity because of strict compliance requirements and evolving regulations that require frequent operational and technical adjustments. Quality expectations, customer and patient demands, highly competitive commercial environments, and the continuous need to innovate and invest in R&D are all additional drivers for modernising operations and improving business processes.

In terms of cybersecurity, the reality is that those who wish to cause harm or achieve financial gain only have to be successful once to cause considerable damage.

As a result, both digital transformation and cybersecurity should be priority areas in the pharmaceutical industry.

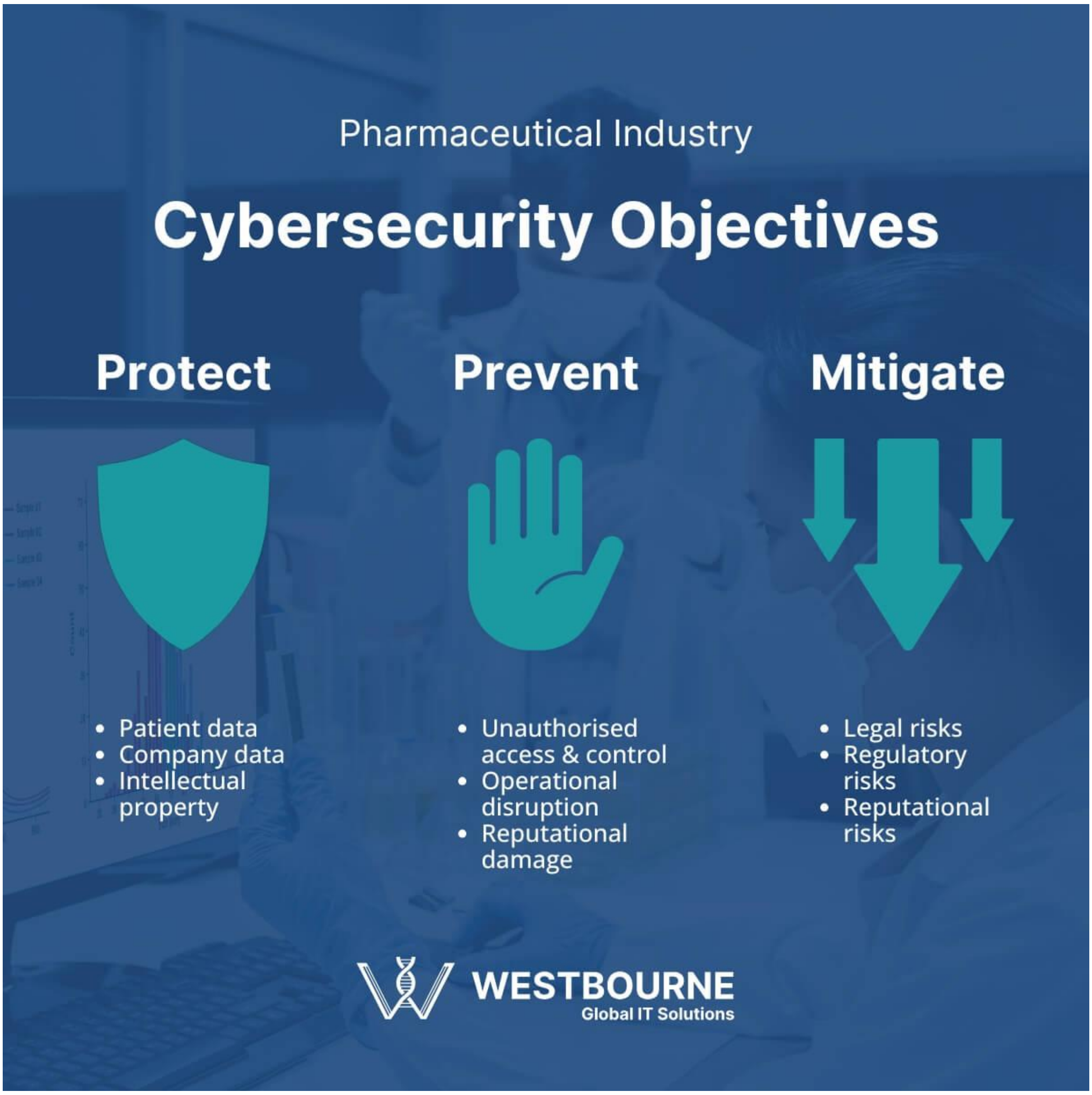
Digital Transformation High Stakes

Digital transformation decisions (projects to green light, technologies to implement, partners to work with, etc) impact operations during and after implementation. Digital transformation decisions also impact the cybersecurity risk landscape.

Key cybersecurity objectives include:

- Preventing unauthorised access and control.
- Protecting sensitive data, both company data and also, potentially, patient data.
- Ensuring patient safety is never compromised.
- Securing intellectual property.
- Preventing operational disruption.
- Mitigating the legal and regulatory risks of cybersecurity breaches.
- Preventing reputational damage.

Nobody wants to implement digital transformation solutions that deliver productivity and other operational benefits on one side while creating cybersecurity vulnerabilities on the other.



Pharmaceutical Industry

Cybersecurity Objectives

Protect

- Patient data
- Company data
- Intellectual property

Prevent

- Unauthorised access & control
- Operational disruption
- Reputational damage

Mitigate

- Legal risks
- Regulatory risks
- Reputational risks

WESTBOURNE
Global IT Solutions

Controlling the Attack Surface

One of the consequences of many digital transformation initiatives is an increase in the size of the potential attack surface. In other words, increasing the potential entry points that malicious actors and cybercriminals can use to get into systems and/or access data.

For example, integration is a crucial component in digital transformation. This is where platforms, systems, and equipment are connected to improve the flow of data. However, each point of connection and every integration has the potential to expose systems and data to cybersecurity vulnerabilities.

We can use the implementation of a new machine as an example. Optimising the potential of that machine might mean giving the vendor remote access so updates can be carried out and performance can be monitored. That connection to the vendor offers operational benefits, but it is also an expansion of the potential attack surface, so it changes the risk equation.

Controlling the potential attack surface is essential, as is implementing risk mitigation measures that block entry points while enabling the operational benefits of digital transformation.

Essential Cybersecurity Considerations

Essential considerations to control the potential attack surface and mitigate cybersecurity risks include:

Ecosystem Complexities

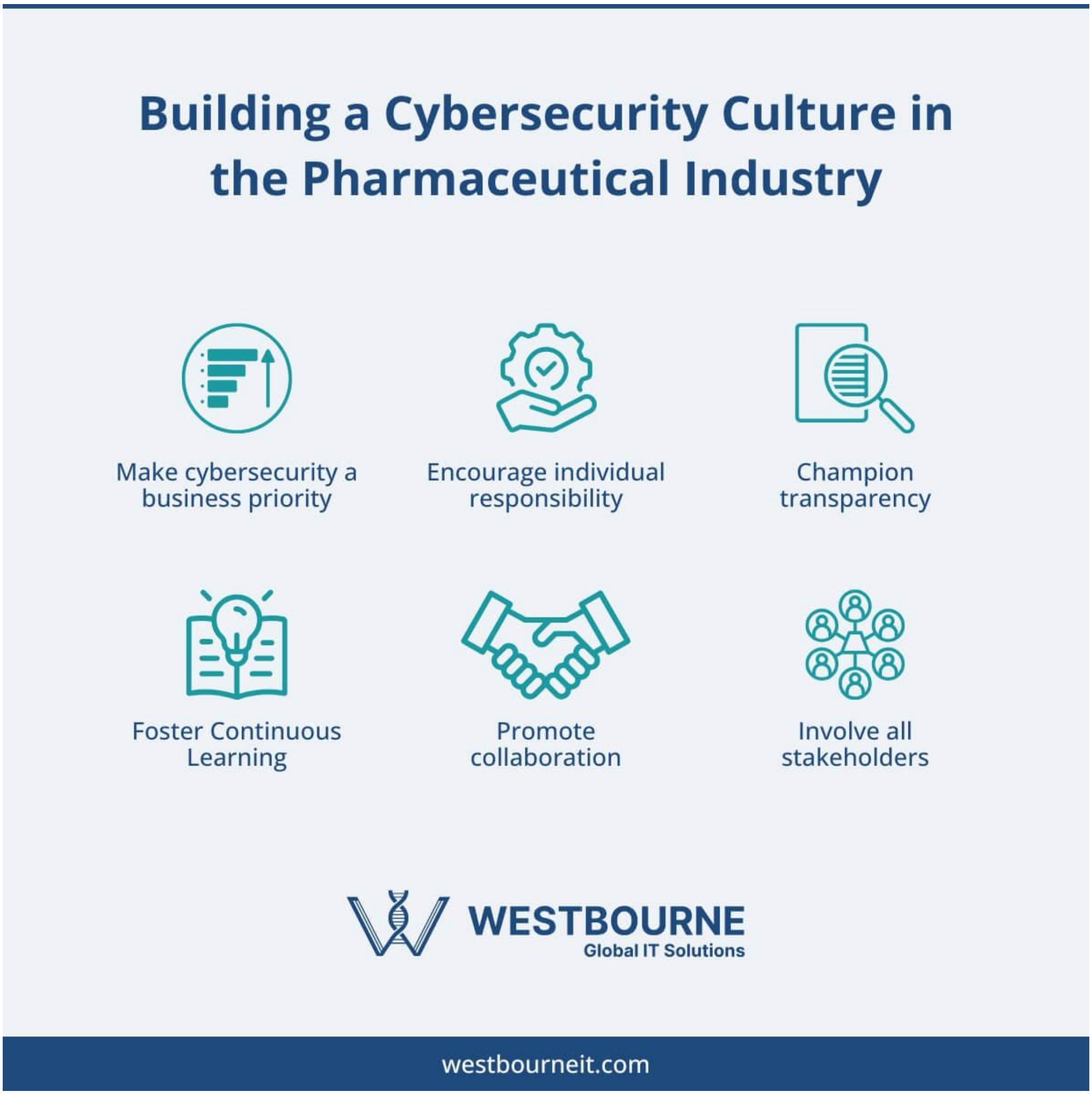
- The presence of legacy systems, especially those that were not originally designed to be connected to other systems, networks, or the internet.
- The complexity of pharma company ecosystems with different technologies and equipment that have often evolved over time.

Operational Complexities

- The complexity of production processes and supply chains.
- The fact that every facility, production line, and laboratory is different.
- The unique nature of pharmaceutical manufacturing and laboratory facilities, especially in relation to patient safety, compliance, and protecting intellectual property.
- The use of contract design and development organisations (CDMOs).

Staffing and Collaboration Challenges

- The need for IT and operational technology (OT) teams to work together.
- The need for staff training and its ongoing importance.
- The benefits of establishing and maintaining a cybersecurity culture.



Building a Cybersecurity Culture in the Pharmaceutical Industry

Make cybersecurity a business priority

Encourage individual responsibility

Champion transparency

Foster Continuous Learning

Promote collaboration

Involve all stakeholders

WESTBOURNE
Global IT Solutions

westbourneit.com

Best Practices

- Conducting regular vulnerability testing and risk assessments.
- Implementing access controls to control access to both systems and data.
- Encrypting data in transit.
- Ensuring update management processes are robust and reliable.

- Implementing and regularly stress-testing backup and disaster recovery procedures.
- Considering cybersecurity factors when vetting and selecting vendors.
- Ongoing monitoring and incident response, including through Security Operations Centres (SOCs).
- Establishing a zero-trust architecture to help protect against cybersecurity threats both from outside and inside the organisation. In a zero-trust architecture, all users and all devices must be authenticated before they get access to systems or data.

Digital Transformation Cybersecurity in the Pharmaceutical Industry

Digital transformation cybersecurity in the pharmaceutical industry is both a macro and micro consideration, i.e., from the smallest sensors and edge devices to the most complex processes, software platforms, and integrations.

Therefore, it is important to work with partners that not only have expertise implementing digital transformation initiatives in the pharmaceutical industry but also have extensive cybersecurity expertise.

We offer all three capabilities at Westbourne – digital transformation, pharmaceutical, and cybersecurity expertise. Get in touch to speak to our cybersecurity experts.