

CYBERSECURITY · LOSS CONTROL · BUSINESS CONTINUITY

Cyberattack Disrupts Boston Scientific

A critical lesson in cybersecurity, loss control and business continuity

DATE 1 SEPTEMBER 2026 PREPARED FOR ICLPSM MEMBERS

CATEGORY INDUSTRY TRENDS · CYBERSECURITY · LOSS CONTROL · BUSINESS CONTINUITY

The recent cyberattack against Boston Scientific, a major global medical technology company, provides an important reminder that cybersecurity is no longer solely an information-technology concern. For modern organisations, cybersecurity has become closely connected to loss control, business continuity, operational risk, corporate security and organisational resilience.

Boston Scientific detected an intrusion into some of its IT systems on 25 August 2026 and disclosed the incident the following day. Nearly one week after the attack, the company was still working to restore normal operations.

The incident disrupted the company's global network and affected important business functions, including product manufacturing, customer order processing and shipping. The company has engaged CrowdStrike and other cybersecurity specialists to assist with the investigation and recovery process.

While the incident occurred within a major international medical technology company, its implications extend well beyond the healthcare sector. It demonstrates how a cyber incident can quickly develop into a wider organisational loss.



DIGITAL RESILIENCE

SECTION 02

Why This Matters to Loss Control and Security Professionals

Traditionally, loss control has often focused on protecting physical assets, preventing theft, reducing fraud, managing operational hazards and protecting people and property.

A successful cyberattack can therefore result in:

- Operational downtime
- Delayed customer orders
- Financial losses
- Regulatory and compliance exposure
- Increased recovery and investigation costs
- Production interruptions
- Supply-chain disruption
- Reputational damage
- Loss of customer confidence
- Disruption of essential services

However, the modern organisation depends heavily on digital infrastructure. A successful cyberattack can therefore result in a broad range of organisational consequences, extending well beyond the IT department itself.

“

Loss prevention must extend beyond physical assets to include digital assets, information systems and technology-dependent operations.

SECTION 03

Cybersecurity and Physical Operations Are Increasingly Connected

The Boston Scientific incident demonstrates the growing connection between cybersecurity and physical business operations. Manufacturing facilities, warehouses, logistics systems, medical technologies and corporate operations increasingly depend on interconnected digital systems.

A cyberattack affecting an organisation's IT infrastructure can therefore have consequences far beyond computers and networks — as the chain below illustrates.



A weakness at one point in this chain can create losses throughout the organisation. This convergence means that security professionals must increasingly understand both physical and digital risk environments. A loss-control assessment that considers only physical security may therefore fail to identify significant areas of organisational exposure.

SECTION 04

Business Continuity Must Be Part of Loss Prevention

One of the most important lessons from the Boston Scientific incident is the importance of business continuity and operational resilience.

Cybersecurity controls are designed to prevent, detect and respond to attacks. However, no organisation can assume that prevention will always be successful.

“

If our critical systems became unavailable tomorrow, could we continue operating?

The objective is not merely to prevent an incident. The objective is also to minimise losses when prevention fails and restore critical operations as quickly as possible.

EFFECTIVE BCP SHOULD CONSIDER

- 01 Identification of critical business processes
- 02 Systems and assets those processes depend on
- 03 Alternative methods of continuing operations
- 04 Data backup and recovery arrangements
- 05 Incident-response procedures
- 06 Communication plans for stakeholders
- 07 Supplier and third-party dependencies
- 08 Recovery Time Objectives (RTOs)
- 09 Recovery Point Objectives (RPOs)
- 10 Regular testing of continuity plans

SECTION 05

The Role of the Loss Control Professional

The role of the modern loss-control professional is evolving. Today's professional increasingly operates at the intersection of the disciplines below.

SECURITY · RISK MANAGEMENT · TECHNOLOGY · COMPLIANCE · LOSS PREVENTION · BUSINESS CONTINUITY

A comprehensive organisational loss-control assessment should therefore consider questions such as:

- ☐ What are the organisation's most critical digital assets?
- ☐ What would happen if these systems became unavailable?
- ☐ Which physical operations depend on digital infrastructure?
- ☐ How quickly could critical systems be restored?
- ☐ Are backups protected against compromise?
- ☐ Are employees trained to identify cyber threats?
- ☐ Are third-party suppliers creating additional exposure?
- ☐ Are incident-response responsibilities clearly defined?
- ☐ Has the organisation tested its recovery plans?
- ☐ Are cyber risks in the wider risk-management framework?

These questions demonstrate why cybersecurity should not operate in isolation from broader organisational security and loss-control functions.

SECTION 06

A Warning for Critical Sectors

The Boston Scientific incident is particularly relevant to organisations operating in sectors where digital disruption can have serious operational and financial consequences. These include:



HEALTHCARE



BANKING & FINANCE



MINING



MANUFACTURING



AGRICULTURE



TELECOMS



ENERGY



TRANSPORT &
LOGISTICS



GOVERNMENT



RETAIL &
DISTRIBUTION

In these environments, a cyberattack can potentially progress from a digital security incident to an operational crisis. For critical sectors, cybersecurity resilience should therefore be treated as an integral component of organisational security and loss prevention.

SECTION 07

What ICLPSM Members Should Take Away

7.1 Cyber Risk Is Business Risk

Cybersecurity failures can directly affect revenue, production, customers, supply chains and organisational reputation — and belong in the wider risk-management and loss-control framework.

7.2 Digital Assets Need Attention

Information, networks, databases, software, cloud systems and connected devices should be incorporated into modern asset-risk assessments.

7.3 Prevention Alone Is Insufficient

Organisations need capabilities across the entire incident lifecycle. A strong organisation continues critical operations even when controls are breached.

PREVENTION

DETECTION

RESPONSE

RECOVERY

CONTINUITY

7.4 Security Must Work Together

IT security, physical security, risk management, compliance, loss control and senior management should not operate in disconnected silos.

7.5 Resilience Must Be Tested

A business continuity plan that has never been tested may provide a false sense of security. Organisations should run exercises and simulations to confirm that their people, systems, procedures and communication channels can actually function during a major disruption.

SECTION 08

Lessons for Organisations in Zimbabwe

The Boston Scientific incident also provides an opportunity for Zimbabwean organisations to reflect on their own exposure — considering what would happen if systems such as these were suddenly unavailable:

- Banking and payment systems
 - Customer databases
 - Production systems
 - Communication platforms
 - Logistics systems
- Payroll systems
 - Inventory systems
 - Access-control systems
 - CCTV and security-management systems
 - Electronic document-management systems

THE OLD QUESTION

“How do we stop cyberattacks?”

THE NEW QUESTION

“How do we minimise organisational losses if our systems are compromised?”

This shift in thinking is fundamental to modern loss control.

SECTION 09

The Growing Convergence of Cyber and Physical Security

The traditional separation between cybersecurity and physical security is becoming increasingly difficult to maintain. Access-control systems may be digitally managed; CCTV systems may operate through networks; industrial equipment may be connected to the internet; warehouses may rely on automated inventory systems; security operations centres may depend on digital communication platforms.

Consequently, compromising a digital system can potentially compromise physical security operations — creating a growing need for professionals who understand the relationship between:

CYBERSECURITY + PHYSICAL SECURITY + RISK MANAGEMENT + LOSS CONTROL + BUSINESS CONTINUITY

This is an important area for continued professional development within the security and loss-control profession.

SECTION 10

Looking Beyond the Incident

The Boston Scientific cyberattack should encourage organisations to reconsider what they define as an "asset" and what they consider a "security incident." In today's interconnected environment, a compromised computer system can become:

- A production problem

A supply-chain problem

A customer-service problem

A financial problem

A compliance problem

A reputational problem

A business-survival problem

“Security must evolve alongside the risks facing modern organisations.”

Cybersecurity is no longer simply about protecting computers. It is about protecting operations, assets, people, information, continuity and the organisation itself.

SECTION 11 · ICLPSM PROFESSIONAL INSIGHT

QUESTION FOR MEMBERS

“

If your organisation's critical IT systems were unavailable for seven days, which operations would stop first — and what controls are currently in place to prevent or minimise those losses?

This question provides a practical starting point for organisations seeking to evaluate their cyber resilience and business-continuity preparedness. The modern loss-control professional should not wait for an incident to expose weaknesses.

IDENTIFY THE EXPOSURE ► ASSESS THE RISK ► STRENGTHEN THE CONTROLS ►
PREPARE FOR DISRUPTION ► PROTECT THE ORGANISATION

**Institute of Chartered Loss Control and Private Security Management**

*Advancing professional standards in Loss Control, Private Security Management, Risk
Management and Organisational Resilience.*

ICLPSM | PROFESSIONAL KNOWLEDGE FOR A CHANGING SECURITY ENVIRONMENT