BlackBerry | Cybersecurity

BLACKBERRY OPERATIONAL TECHNOLOGY INSIGHT GUIDE FOR

OPERATIONAL TECHNOLOGY ENVIRONMENTS

BlackBerry | Cybersecurity

Contents

Introduction	3
Challenges in Securing Manufacturing Environments	4
The Growing Cyberthreat	6
Enhancing and Securing Operational Resilience	7
The BlackBerry Approach	8
Harnessing Smarter Insights to Detect Attacks	9
Helping an Energy Provider Secure Online and Offline Environments	10

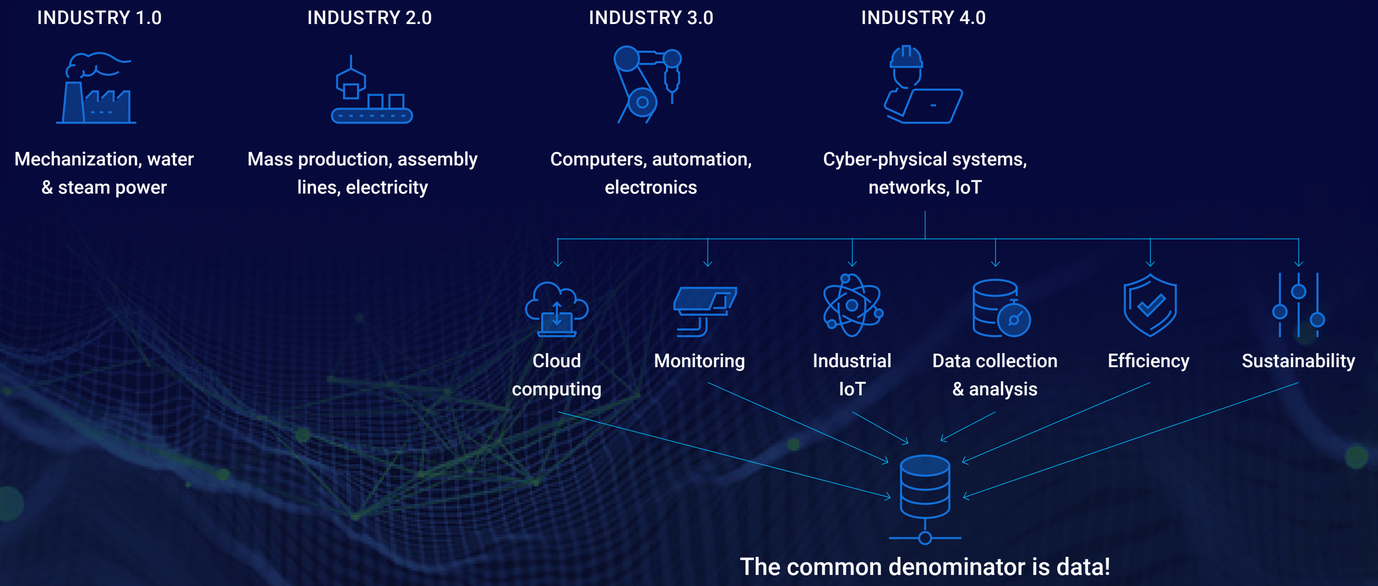
Introduction

Born out of the common challenge for the need to connect and access real-time insights across process, people and products, with a view to make data actionable, Industry 4.0 is shaping the future of manufacturing environments. As we progress through the age of Industry 4.0, manufacturing facilities have already gone through a vast transformation to modernise their environments and create a more data-driven approach to operations. While these transformations can add value through enhanced productivity, enabling more intelligent insights and driving smarter decisions, they are not without risk.

The increasing use of innovative operational technologies (OT) such as automation, IoT devices and robotics in today's modern manufacturing environments combined with devices running on legacy operating systems that are air-gapped from the IT infrastructure and working in silo bring challenges around operational resilience.

The IBM X-Force Threat Intelligence Index 2022[1] found that manufacturing has become the world's most attacked industry outpacing finance and insurance for the first time in 5 years. Ever evolving cyber security threats together with industry challenges are leaving manufacturing organisations vulnerable to attack. The industry's low tolerance for downtime and the significant impact an attack could have on revenue means these vulnerabilities simply cannot be ignored.

As manufacturing moves towards digitisation and automation, this paper explores the key challenges organisations face and looks at how adopting a prevention-first approach can help build and secure operational resilience no matter where you are on your journey to Industry 4.0.



[1] Source: https://www.ibm.com/security/data-breach/threat-intelligence/

Challenges in Securing Manufacturing Environments

Manufacturing environments are often unique from a technology perspective. From running legacy devices and systems to insufficient security measures and growing connectivity to the internet creating more vulnerabilities. Combine this with the shortage of operational technology security skills and the increasing risk of supply chain attacks, and it's easy to understand why the manufacturing sector has become a prime target for threat actors.

Reliance on legacy devices and systems

The vast majority of manufacturing environments operate older devices, protocols and operating systems such as Windows® XP, which often splits into two scenarios. Ones that are connected to the Internet but not patched and updated so therefore are not protected and create a greater security risk and those which are air-gapped from IT infrastructure, are incapable of cloud connectivity and work in silo.

The upgrade path for such devices and systems is often limited as the associated costs, risk of downtime and loss of productivity prohibit upgrades from being viable, but little or no security measures on the devices further expands the attack surface and makes it increasingly difficult to secure the environment should they be compromised.

Moving towards digitisation and automation

With greater levels of digitisation comes greater levels of risk. As the industry continues to transform its environments and the use of automation, IoT devices and robotics grows, so does the attack surface. While innovative operational technologies drive productivity and therefore revenue, the impact on downtime as a result of an attack could quickly soar to millions of pounds of loss. Add into the mix that this creates a growing dependence on third-party vendor software, which is typically locked off, and manufacturing organisations can quickly no longer be in full control of their environments.

Security skill shortage in the OT space

One of the most significant challenges in the operational technology space is the security skill shortage. While IT and OT security skills are transferable the philosophies differ somewhat. The differences come in the approaches, IT would come from the view of taking systems down to contain and respond to an attack whereas the OT perspective would be to mitigate downtime and loss of revenue.

Conflicts in approaches and cultures can create challenges when it comes to OT security, challenges which are further compounded by a younger workforce being unfamiliar with older technology, operating systems and practices.

Increasing supply chain attacks

Vulnerabilities in the digital supply chain are also becoming a growing concern across the industry. Third-party dependency creates greater exposure to vulnerabilities, not only are manufacturing environments restricted to the vendors software and limited control of it but there is also a risk that the software could have been compromised and preloaded with malware that enables threat actors to remotely access and take control of industrial control systems.

The challenge for organisations, in light of growing legal liabilities and regulatory enforcement, is to utilise solutions that are easy to install, minimise possible security risks and enable production to keep flowing.

> “All industries are distinct in their operational focus, many with extensive physical infrastructures, that requires the development of a bespoke systematic approach to assessing and maintaining the security posture of their ICS systems, including legacy architectures, legacy systems, and legacy devices, without replacement.”
>
> **Hans-Peter Bauer,** Senior Vice President - EMEA Sales, Cybersecurity

The Growing Cyberthreat

Understanding the vital role manufacturing plays in supply chains around the world, threat actors have concentrated their focus on the industry to impact industrial processes, gather valuable data and process information theft to cause as much disruption as possible and increase the chance of ransoms being paid.

Manufacturing is now the most attacked industry, and it is anticipated that as we continue through the age of Industry 4.0 the prevalence and sophistication of attacks will grow exponentially. Utilising their deep understanding of the vulnerabilities within the industry and how to exploit them is helping malicious attackers compromise operational technology and cause disruption and downtime across manufacturing environments.

In addition to ransomware, recently observed TTPs include spear phishing, compromising Internet-accessible programmable logic controllers (PLCs) requiring no authentication for initial access and the use of third-party vendor engineering software and program downloads to gain access to the operational technology and industrial control systems via preloaded malware.

The current outlook

2,000%

rise in incidents targeting operational technology & industrial control systems in 2020[2]

1 in 4

cyber attacks in the manufacturing sector are from ransomware

47%

of attacks in manufacturing got in through vulnerability exploitation

1,897 days

is the average vulnerabilities exist “in the wild” (5.2 years) and 8,152 days in the worst case.

[2] Source: IBM X-Force Threat Intelligence Index 2020 - Page 5

BlackBerry | Cybersecurity

Enhancing and Securing Operational Resilience

Recognising the growing threat to the industry, leading manufacturing organisations are beginning to accelerate their operational technology security. Many incorporating it into their enterprise risk management efforts by adopting an end-to-end security solution that can help prevent, detect and respond to attacks as well as strengthen their defences against supply chain attacks.

Is your supply chain or ICS environment vulnerable?

Prepare

A compromise assessment can help organisations identify security gaps and report effective remediation steps.

Prevent

Continually monitor systems, networks, devices, personnel and the environment for possible threats both online and offline.

Respond

Create a detailed incident response plan to minimise the impact of an incident should a breach occur.

"The increase in cyberattacks targeting industrial networks and systems is growing exponentially, making cybersecurity in manufacturing more important than ever.

However, cybersecurity should not be driven solely by fear, but seen as a competitive advantage that leads to having secure, reliable and trustworthy products and services, that act as an enabler of business opportunity."

Hans-Peter Bauer, Senior Vice President - EMEA Sales, Cybersecurity

The BlackBerry Approach

The BlackBerry end-to-end approach is centred on providing context with regard to the potential business impact of cyberthreats. By applying a structured and methodical approach to security, BlackBerry experts will map out the different types of threat actors, their potential entry points, detection points, as well as prevention and containment opportunities within your networks and offline systems.

We discuss ways to protect legacy architectures, legacy systems with outdated operating systems and legacy devices to prevent malicious threat actors from shutting down your grid and halting your business operations.

Why Prevention-First?

While a reactive approach is common across all industries, it is particularly prevalent in the manufacturing industry. Combing the challenges of the industry, the increasing rise in supply chain attacks and the ever-evolving cybersecurity threats, manufacturing organisations must consider the preventative actions they can take to ensure they remain productive, profitable and protected.

At BlackBerry, we take a prevention-first approach to stop attacks at the door. Our lightweight solutions are designed to place the right technology in the right place to stop malicious activity from getting anywhere near networks and run with minimal CPU space and without impact to business critical functions. They continuously analyse changes occurring on the endpoints to uncover threats, that would be difficult if not impossible, for a human analyst to find quickly enough to mitigate. Adopting a prevention-first approach can help reduce the risks of downtime, minimise business disruption and mitigate the risk of financial loss.

> “One of the chief benefits of BlackBerry in the industrial control systems space is our ability to ensure a preventative state without having to constantly update the endpoint agent or rely on cloud connections. This is of particular value for offline endpoints and air-gapped networks, but the benefits go deeper.”
>
> **Nathan Jenniges,** Vice President of Product Strategy, Cybersecurity

BlackBerry | Cybersecurity

Harnessing Smarter Insights to Detect Attacks

At BlackBerry, we have a long history of securing communications, productivity and work life. Our solutions and software are deployed across a wide range of manufacturing facilities and industrial control systems to secure operational resilience and harden the security posture by ensuring always-on protection whether the device is online or offline.

Our end-to-end approach to cyber security is deeply rooted in Cylance® AI and machine learning to provide enhanced visibility and protection against current and future cyber threats. Without the need for human intervention or constant updates, our portfolio of Cylance solutions delivers greater stability in IT systems and secures operational resilience.

CylancePROTECT®

AI-based Endpoint Protection Platform (EPP) that prevents breaches and provides added controls to ward off sophisticated cyber threats even without human intervention.

CylanceOPTICS®

AI-driven Endpoint Detection and Response (EDR) that works with CylancePROTECT® to keep you ahead of cyber attackers and your business secure—even when devices are offline.

Get expert insight to defend against threats to your endpoints. Gain visibility to attacker TTPs, Indicators of Compromise and manage end-user account integrity through a single interface.

Why BlackBerry

- Detects and prevents potentially harmful code in less than 50 milliseconds. Because preventing a breach is faster and more effective than remediating after one.
- Works online and offline. Other cybersecurity providers require code pushes to update endpoints against new cyberthreats. Cylance AI isn't limited by connection status. It requires minimal updates and even works offline.
- Support business objectives while maintaining safe and uninterrupted operations with security.
- Create remediation strategies while balancing risk and return.
- A prevention-first methodology that removes the noise in environments and allows focus on the activities that can be truly harmful.
- Continuously analyzes changes occurring on endpoints, uncovering threats that would be difficult, if not impossible, for a human analyst to find quickly enough to mitigate

Helping an Energy Provider Secure Online and Offline Environments

The CylancePROTECT® endpoint agent sits on the ICS endpoint and provides 99% efficacy[3] against known and unknown attacks in both online and offline environments. One example is where BlackBerry worked with an energy provider who was looking for a strategy to manage its power stations that had systems dating back 40 years, that all required securing. These included industrial control systems, managing process control and a number of laptops that were used to program PLC's.

The customer installed CylancePROTECT as these licenses could be deployed to secure air gapped systems, and in this instance used in disconnected mode on unmanaged endpoints with a standalone network that had no connection to the main corporate network. To enable threat monitoring one carefully selected endpoint was connected online.

CylancePROTECT enabled the business to install an antivirus product where others that required regular virus updates and signature files updates were simply not practical. The approach has been positively recognised by the Office for Nuclear Regulation when reviewing the providers cyber security provision.

The safety, regulatory and commercial demands of today's energy providers are such that addressing new cyber attack challenges with old solutions is no longer viable. At the same time, protecting the endpoint – whether online or off – is only part of the puzzle. A comprehensive strategy is needed to deliver the assurance to do business in confidence.

For more information on how Blackberry can help secure your OT environments and defend against sophisticated cyberattacks, contact us.

[3] Source - https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/wp-protect-nss_labs-advanced-endpoint-protection.pdf

BlackBerry Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 215M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry | Cybersecurity