BlackBerry Intelligent Security. Everywhere.

UNDERSTANDING CYBERSECURITY RISKS TO MANUFACTURING INFRASTRUCTURE

WHITE PAPER

SUMMARY

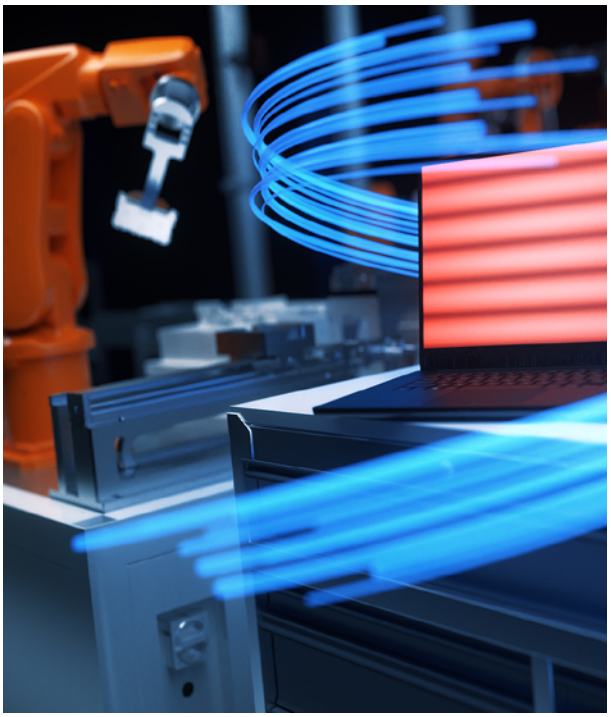
The global manufacturing industry currently confronts a growing risk of serious cybersecurity incidents. This research into the sector reveals key threats to operational technology. It also uncovers several potential barriers to creating a more secure shop floor.

In the context of recent political instability, anxieties about cyberattacks by nation-states loom large. Across the sector, there is an increased appetite for investment in cybersecurity protections.

Yet the financial impact of cyberattacks is underestimated. Within manufacturing, IT decision makers' predictions about the cost of recovering from a cybersecurity breach are much lower than the true cost. Manufacturers struggle to understand the extent of the issues they face.

The Operational Technology (OT) infrastructure on which manufacturing relies is proving harder for organizations to defend than conventional IT infrastructure. A complex security landscape compounds the problem.

Organizations are attempting to protect critical assets by segmenting OT and IT systems with security protocols. Nevertheless, the sector's widespread habit of combining legacy production processes with current technology makes infrastructure increasingly vulnerable to cyberattacks.



Industrial equipment is built for decades of use, meaning that operating systems typically lag far behind the update cycle of modern software. A shocking number of organizations rely on outdated and unsupported operating systems to perform core functions.

For those organizations undergoing digital modernization, adopting more sophisticated solutions may only increase the complexity of their security requirements.

ABOUT THE STUDY

BlackBerry asked 1,500 senior IT decision makers and cybersecurity leaders in the manufacturing sector about the cybersecurity risks they face.

The respondents come from the US, the UK, Germany, Japan, Australia and Canada. They belong to organizations which range in size from fewer than 100 employees to 17,500. The average annual revenue of their workplaces is $277 million.

Their titles include Head of IT, Chief Technology Officer, Director of Threat Intelligence, and Chief Information Officer. They work for manufacturing organizations supplying computers, consumer electronics, electrical equipment, industrial equipment, clothing, healthcare, food and agriculture, chemicals, furniture, oil and gas and in the automotive industry.

KEY FINDINGS

71% of organizations in the manufacturing sector have been subjected to a cybersecurity incident in the past year

Almost three quarters of organizations surveyed in the manufacturing sector have been targeted by a cyberattack. This includes incidents arising from employee errors.

- 41% of survey respondents predict that the risk of cyberattack will rise in 2023

Across the sector, concerns about cybersecurity are growing, leading organizations to invest more in defending themselves from threats.

- 75% of IT decision makers in manufacturing believe that other nation-states are actively targeting manufacturers in their country at this time

Manufacturers fear being targeted by state-sponsored actors who might seek to damage critical assets, steal information or spy on their activities.

- 68% say that Operational Technology (OT) infrastructure poses different risks and is more difficult to defend than IT infrastructure

The technology used on the shop floor, at the center of production, is the vulnerable core of the manufacturing sector.

- 86% of manufacturing representatives admit to running core functions on outdated and unsupported legacy operating systems

The majority of manufacturers are dependent on operating systems that are no longer supported by their creators, meaning that they have no active inbuilt security defenses. For example, 37% of manufacturers still use Windows NT within their operational technology environment, an operating system that was last supported 19 years ago in 2004.

MANUFACTURING TARGETED BY CYBERATTACKS

Cyberattacks are ubiquitous across the manufacturing sector. Throughout organizations in North America, the UK, Germany, Australia, Japan and Canada, 71% of senior IT decision makers reported that they had been hit by a cybersecurity incident in the last 12 months. The figure was highest in Germany, where 78% of organizations had been subject to a cyberattack.

Insiders recognize that risks are rising across the sector, with 41% predicting that the threat of cyberattacks will increase in 2023. Over half of manufacturers (56%) plan to invest more spending on cybersecurity this year.

28% surveyed believe they would not be able to achieve their business goals for 2023 if they experienced a major cybersecurity incident over the course of the year

Cybersecurity leaders across manufacturing understand that attacks can severely impact organizations. Over a quarter of those surveyed (28%) said that they would not be able to achieve their business goals for 2023 if they experienced a major cybersecurity incident over the course of the year. 63% recognized that if a cyberattack impacted their operations, they would likely lose customers. 59% were concerned that their relationship with suppliers would be damaged.

THE TRUE COST OF CYBERSECURITY INCIDENTS

The financial impact associated with cybersecurity incidents is high. 71% of organizations estimated that in the event of a cyberattack, the cost of an interruption to their manufacturing operations would be more than $10,000 per hour of downtime. 20% predicted that downtime would cost between $25,000 and $50,000. The average time it would take to get back up and running was reported to be eight days, with 12% saying it would take more than three weeks.

On average, manufacturers estimated that the total cost of a cyberattack on their organization would be $250,000. Yet this may be a significant underestimate. A recent report estimated the cost of a cybersecurity incident to be $4.45[1] million—more than 7 times higher than the average figure given by survey respondents.

The impact of a cybersecurity incident amounts to more than business downtime. The cost of recovery is far greater. In the aftermath of a cyberattack, organizations must restore and update their technological infrastructure, and absorb the impact of lost production, and the knock-on effect to their reputation.

A COMPLEX THREAT LANDSCAPE

Why does the manufacturing sector consider itself a primary target of cyberattacks? When it comes to cybersecurity threats, manufacturers share common concerns.

75% of IT decision makers in manufacturing believe that other nation-states are actively targeting manufacturers in their country at the current time. 65% report that they are concerned about foreign governments spying on manufacturing facilities. For example, according to recent research by BlackBerry and Make UK, manufacturers in the UK are primarily worried about state-sponsored actors in Russia and China[2].

Manufacturers fear state-sponsored actors may be infiltrating manufacturing systems for the purpose of espionage, to damage critical assets or to steal information. They suspect these activities may be motivated by geopolitical hostilities, or the desire for competitive advantage.

However, this focus on state-sponsored actors does not do full justice to the complex threat landscape manufacturers face. Ransomware attacks, which target organizations to extort money, can and do shut down factories, wreaking havoc across organizational supply chains.

A ransomware attack on an organization's information technology (IT) system, designed to extort money, interrupt operations, or destroy assets, may also severely impact its Operational Technology (OT) environment. For many manufacturers, IT and OT systems are interdependent, so a breached IT system has major ramifications on the shop floor.

THE MOTIVATIONS BEHIND CYBERATTACKS

The manufacturing sector faces cybersecurity threats from attackers motivated by a variety of different goals.

ESPIONAGE

The goal of these cyberattacks is information-gathering. In manufacturing, organizations may be targeted by attackers seeking cutting-edge techniques that bestow a competitive advantage. Some attacks may be perpetrated by nation-states seeking industry knowledge.

One recent example is the NewsPenguin malware, which targeted government organizations and manufacturers attending a maritime technology conference in Pakistan early this year. The NewsPenguin phishing campaign sought information about maritime and military technologies[3].

DESTRUCTION

Sometimes, cyberattackers seek to destroy a target by interrupting critical functions. These attacks might be carried out by state-sponsored actors or by "hacktivists."

For example, during the ongoing conflict in Ukraine, the country has suffered a surge in cyberattacks, some resulting in major interruptions to energy providers. Hackers such as NoName057(16) have also targeted Ukraine's allies. Malicious software that seeks to delete data, known as "wiper" malware, is on the rise.

EXTORTION

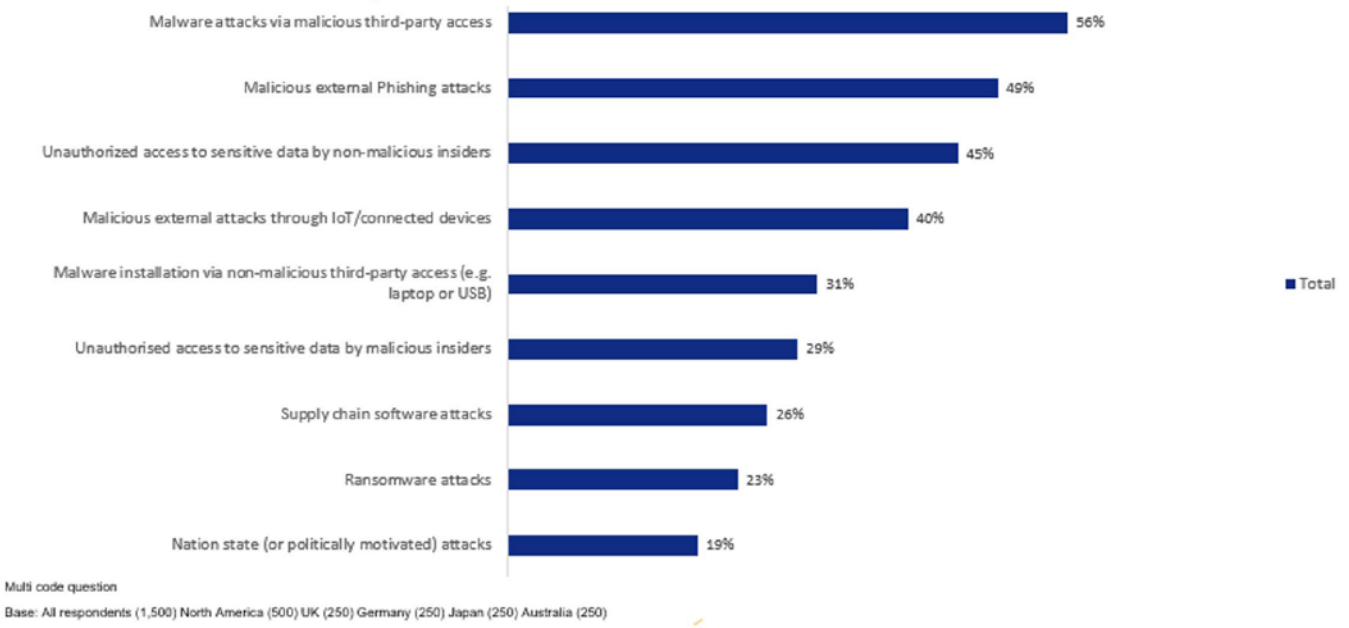
Some cyberattacks are motivated by financial gain, for example, by seeking to extort a ransom from victim organizations. Attackers threaten to disable their target's operations, or publish confidential information, unless they are paid off.

In 2017, WannaCry ransomware targeted organizations around the world, infiltrating unsupported versions of Microsoft Windows. It encrypted data and demanded a ransom for its release. Manufacturers around the world were attacked, as was the UK's National Health Service.

MANUFACTURERS' GREATEST FEARS

Organizations were asked what they considered their main threats were to their Operational Technology (OT) infrastructure.

Q.8. What do you consider to be the main cybersecurity threats to your manufacturing OT infrastructure at the present time?



When senior IT decision makers in manufacturing were asked to select the greatest threats to their organization, 56% chose malware attacks through malicious third-party access, and 49% chose malicious phishing attacks (where attackers tempt users to do the wrong thing, such as clicking on an email link that downloads a malicious file.)

Their concerns about intentional attacks included malicious attacks through connected devices including via the Internet of Things (40%), followed by unauthorized access to sensitive data by malicious insiders (29%), ransomware attacks (23%), and politically motivated attacks (19%).

There's a noticeable difference between the respondents' awareness of widespread politically motivated attacks (see "A complex threat landscape") and their optimistic belief that these attacks will not target them specifically, pushing this threat to the bottom of the list.

After intentional malware and phishing attacks, respondents were most concerned about a different type of infiltration—one without malicious intent behind it. 45% were worried about unauthorized access to sensitive data by non-malicious insiders. 31% also named malware installation via non-malicious third-party access (e.g. laptop or USB) as a potential risk factor.

This may reflect the fact that across the manufacturing sector, operational technology is typically protected through systems of isolation, either by securing physical access to infrastructure or by network segmentation. As a result, non-malicious insiders pose almost as significant a security threat as external attackers, highlighting the vulnerability of these systems.

VULNERABLE INFRASTRUCTURE

68% of manufacturers agreed that complexities in the security landscape make it hard to keep up. However, falling behind may leave their organizations more vulnerable to threats. The problem is compounded by the manufacturing sector's reliance on Operational Technology (OT) infrastructure. 68% of insiders agreed that Operational Technology (OT) infrastructure poses different risks, and is more difficult to defend, than their IT infrastructure.

Within the manufacturing sector, many employees may never touch a computer, as the machinery on the factory floor is run by technology such as controllers and actuators. Humans and machines interface through integrated control panels, engineering workstations, diagnostic laptops and mobile tablets.

However, a shocking finding of this research was the extent to which manufacturers rely on outdated operating systems at the core of production processes.

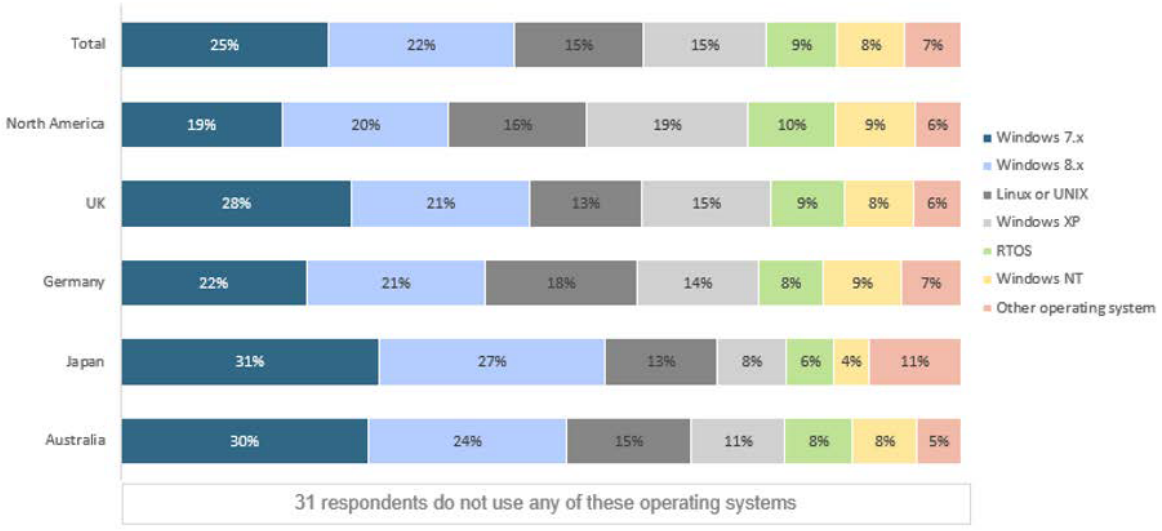
Industrial equipment is built to last for decades, and replacing it is a significant financial outlay. As a result, a factory floor often relies on operating systems that are so antiquated that they are no longer supported by their creators. These operating systems have not been secured for years, and, in some cases, decades.

ANCIENT OPERATING SYSTEMS

95% of respondents needed to update or patch legacy operating systems deployed within their manufacturing infrastructure once a month or more, in order to repair vulnerabilities. Almost half (42%) do so a minimum of several times a week, including 16% who do so daily.

70% of cybersecurity leaders across the manufacturing sector reported that aging hardware limited their ability to update their operational technology.

Q16. Which of the below operating systems are still functional in your Operational Technology (OT) environment?



Percentage

Base: All respondents (1,500) North America (500) UK (250) Germany (250) Japan (250) Australia (250)

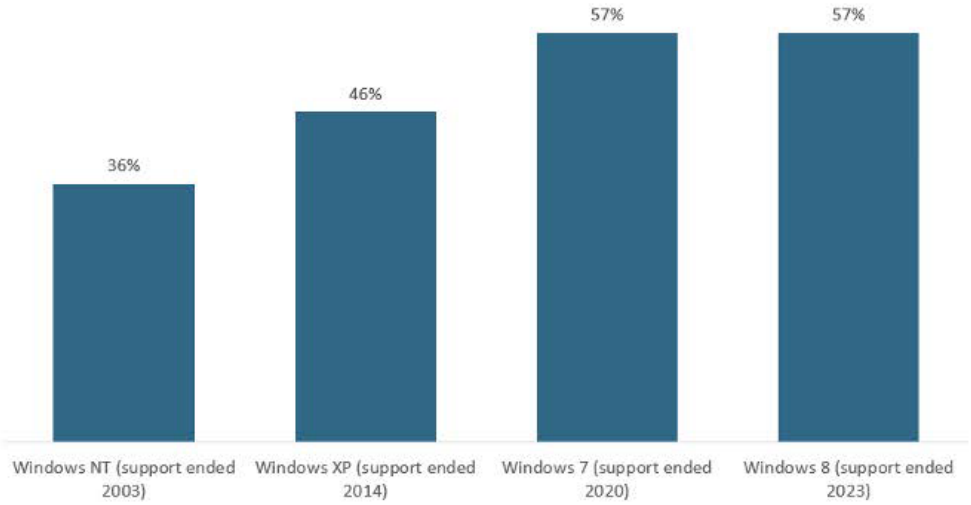
86% of the manufacturing representatives surveyed admitted to running core functions on outdated and unsupported legacy operating systems. These operating systems are no longer managed by their creators, meaning that they have no inbuilt active security defenses. For many organizations, more than one outdated operating system is embedded in their core infrastructure.

36% of manufacturers use Windows NT (first released in 1993), an operating system that was last supported 19 years ago.

36% of manufacturers use Windows NT (first released in 1993), an operating system that was last supported 19 years ago.

46% contain Windows XP (2001), for which support ended almost nine years ago. 57% contain Windows 7 (2009), for which support expired three years ago. And 57% of those surveyed run Windows 8 (2012) in their environments, for which support finished in January 2023.

Q16. Which of the below operating systems are still functional in your Operational Technology (OT) environment?



Percentage
Base: All respondents (1,500)

It may be that however ancient they are, these operating systems will only be updated when the machinery running them dies. With no ability to defend themselves, they can only be protected by other security components deployed in the manufacturer's infrastructure.

49% *of respondents said their operational technology was capable of only limited cybersecurity*

Worryingly, 46% of survey respondents stated that they relied on network wide system and software updates to prevent cybersecurity incidents. In the case of outdated operating systems, such updates are not available. If any vulnerabilities are discovered in these operating systems, they can't be patched: organizations must rely on isolating the network, or on non-patch mitigations, such as configuration changes, to reduce the possibility of attack.

CONTROLLING ACCESS

Alongside system updates, organizations in the manufacturing sector resort to a range of tools and techniques to prevent cyberattacks across their organizations. 62% control access to electronic data and systems. 56% use secure settings across devices and software. 52% use antivirus software, and 30% use firewalls to secure their internet connection.

However, almost half (49%) said that their operational technology was capable of only limited or basic cybersecurity. 40% reported that their Operational Technology (OT) infrastructure was capable of intermediate-level cybersecurity, including monitoring of endpoint and network anomalies, and proactive hardening (eliminating possible attacks in advance). Only 11% said that their organization's Operational Technology (OT) infrastructure capabilities were advanced, involving highly automated artificial intelligence or machine learning, and strong security hygiene practices.

When seeking to protect the critical manufacturing infrastructure at the core of their operations from external threats, the majority of organizations rely on techniques that minimize access to these systems, and/or segment them from the rest of the network. This reflects the anxieties reported about insiders accessing sensitive data with no malicious intent (see Manufacturers' Greatest Fears, above).

It seems to be a last resort for manufacturers whose infrastructure contains especially vulnerable, antiquated operational technology, with no inbuilt protections of its own.

56% of those surveyed said they relied on secure physical access on their premises, and 50% implement access controls, meaning that systems can only be accessed by authorized parties. 36% limit the use of removable media, such as USBs.

47% implement network segmentation and 23% use an air-gapped network, in which protected systems are not connected to any network.

Manufacturers varied a great deal in the way they managed access to isolated networks, and some took more than one approach across their infrastructure. For some, networks weren't segmented at all: 41% said that they were fully open to the internet, and could be directly connected to by a remote user. Ironically, for some organizations, it may be necessary to stay connected to the internet in order to utilize cybersecurity software.

At the other end of the scale, 36% used a segmented network, with on-premise access only. 47% required physical access only, using a portable device directly connected to the machines for control or diagnostics. 52% had set up a gateway, or bridge, between the network for general use and a secure manufacturing network.

When asked how effective the isolation of the manufacturing floors was in preventing external threats, 37% said it was extremely effective, 43% said it was fairly effective, and 20% said it was not very effective or not at all effective.

THE PURDUE MODEL

The most popular approach to segmenting networks among those surveyed was the use of a gateway between the general network and the secure manufacturing network. This is known as the Purdue model. This architecture was conceived of as a completely closed-off system with a rigid hierarchy. A key aspect of the model is a boundary between OT and IT systems. Where no interconnect between the two exists, this is referred to as an "air gap".

However, as organizations increasingly require real-time OT data, and make use of cloud-based systems and services, the model tends to involve more interconnectivity. Administrators use firewalls to connect OT and IT systems, mediating communication between them.

DEFENDING ENDPOINTS

Endpoints are the physical devices that connect to a computer network. They might include desktop computers, mobile devices, virtual machines and servers.

When defending endpoints, 52% of manufacturers said they were most concerned about cybersecurity threats. 17% reported that their main concern was legacy system performance, reflecting the difficulty of connecting older systems with more up-to-date technologies. 14% named connectivity, and the lack of effective isolation and controls, as their main concern when defending endpoints, indicating that they might prefer to shield vulnerable components of their system by means of segmentation.

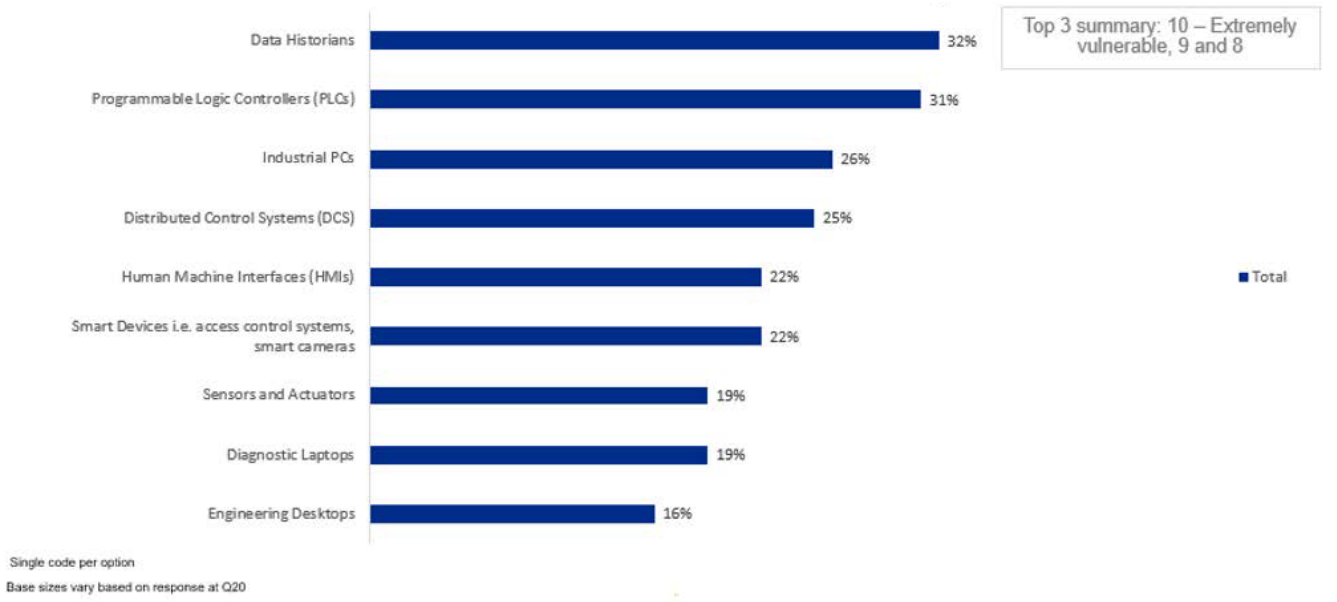
Smaller groups referenced risks from human error due to lack of training or skills (11%) and the need to minimize downtime to ensure operational continuity (6%).

Manufacturers named data historians, databases that log process and production data, as the endpoint most vulnerable to external threats (32%). More than 50% of respondents proactively managed these endpoints more than once a week.

This was followed by programmable logic controllers, industrial devices that make logic-based decisions for automated processes or machines based on inputs and outputs (31%). 38% of respondents managed these several times a week or more.

When defending endpoints, 52% of manufacturers said they were most concerned about cybersecurity threats

Q22. How vulnerable to external threats are each of these endpoints?



FUTURE CHALLENGES

In a rapidly changing technological landscape, manufacturers are increasingly vulnerable to cybersecurity threats. At present, the majority of operational technology within manufacturing organizations is not notably sophisticated. 30% of insiders report that basic manufacturing processes are automated. 29% say that manufacturing machines are connected, and data is shared. 24% of organizations go further, collecting data from manufacturing machines and analyzing it to provide real-time insights. In only 17% of organizations does operational technology involve autonomous decision-making by manufacturing machines, based on data analytics and artificial intelligence.

However, as operations become increasingly connected and automated, manufacturers report emerging vulnerabilities. The top three digital technologies adopted by businesses that have prompted them to take greater action on cybersecurity are artificial intelligence (named by 62%), the industrial Internet of Things (53%) and augmented and virtual reality (40%).

61%

of respondents said their greatest barrier to modernization was cost

44%

of respondents said cybersecurity concerns were also a barrier to modernization

Survey respondents disclosed that their operational technology environments had already begun to adopt modernization strategies, including migration to cloud-based solutions (56%), adoption of the Internet of Things (46%), and integration with modern software and hardware (37%). Over the next five years, 52% said they would implement edge computing, and 37% said they would adopt the use of digital twins.

The greatest barrier to modernization initiatives was named as cost (61%), closely followed by difficulties with data integration (52%). The final leading factor was cybersecurity concerns (44%).

Just 58% of cybersecurity experts in manufacturing were aware of Industry 4.0, the term used to denote the approaching technological revolution in the sector. Industry 4.0 is expected to disrupt manufacturing environments with factors such as increased reliance on data and connectivity, interaction between humans and machines, and improvements in robotics.

Of those who were aware of it, 90% stated that they were aligning themselves with Industry 4.0 developments. The top three concerns, in reverse order, were data security / privacy (38%), interoperability between existing devices and systems (45%) and finally, in the lead at 65%, increased exposure to, and risk of, cyberattacks.

THE SELF-DEFENDING MANUFACTURING FLOOR

BlackBerry sets out to address the unique cybersecurity risks and challenges facing manufacturers with Cylance® Endpoint Security.

It's an AI-based, ultra-lightweight agent designed to protect the lifeblood of your business. Cylance Endpoint Security does not require online access or disruptive updates.

Whether your operational technology systems are air-gapped, connected, or somewhere in between, Cylance® Endpoint Solutions from BlackBerry eliminate complexity, deliver proven security, and enable continuous learning.

BlackBerry can help you establish a self-defending manufacturing floor, delivering a lightweight presence on your endpoints—without the need for signatures, heuristics, or even internet connections.

SUPPORT FOR LEGACY AND AIR-GAPPED SYSTEMS

We offer the market's broadest support for legacy OT systems, ensuring that older mission-critical assets and air-gapped environments are protected.

MAXIMUM UPTIME

AI-based security—always running and up-to-date—minimizes routine interruptions for updating files as well as disruptions due to active threats. Our solution eliminates the need for signature file updates and reduces downtime to support ongoing operational continuity.

MINIMAL IMPACT ON PERFORMANCE

Our agent is ultra-lightweight and designed to deliver complete endpoint security without affecting operations—even on older systems.

SUPERIOR OFFLINE PROTECTION

Air-gapped environments receive the same protection as online environments.

EASY MANAGEMENT

A single management console simplifies security setup and maintenance. Our solution streamlines investigation and reduces noise and "alert fatigue"—so staff can quickly and easily understand and respond to threats.

SCALABILITY

We offer solutions that scale and expand to continually protect vital assets as your manufacturing technologies change and grow, without the need to rip and replace.

Cylance Endpoint Security enables manufacturers to establish a self-defending manufacturing floor. Protect critical data and enable digital transformation without disrupting operations with BlackBerry cybersecurity solutions—powered by Cylance® AI.

[1] IBM Security Cost of a Data Breach Report 2023
[2] https://www.blackberry.com/us/en/company/newsroom/press-releases/2022/blackberry-make-uk-research-reveals-uk-manufacturing-sector-under-threat-as-almost-half-suffer-cyberattack-in-the-last-12-months
[3] https://blogs.blackberry.com/en/2023/02/newspenguin-a-previously-unknown-threat-actor-targets-pakistan-with-advanced-espionage-tool

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 over 235M vehicles. 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, endpoint 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**.*

BB23 | 230417