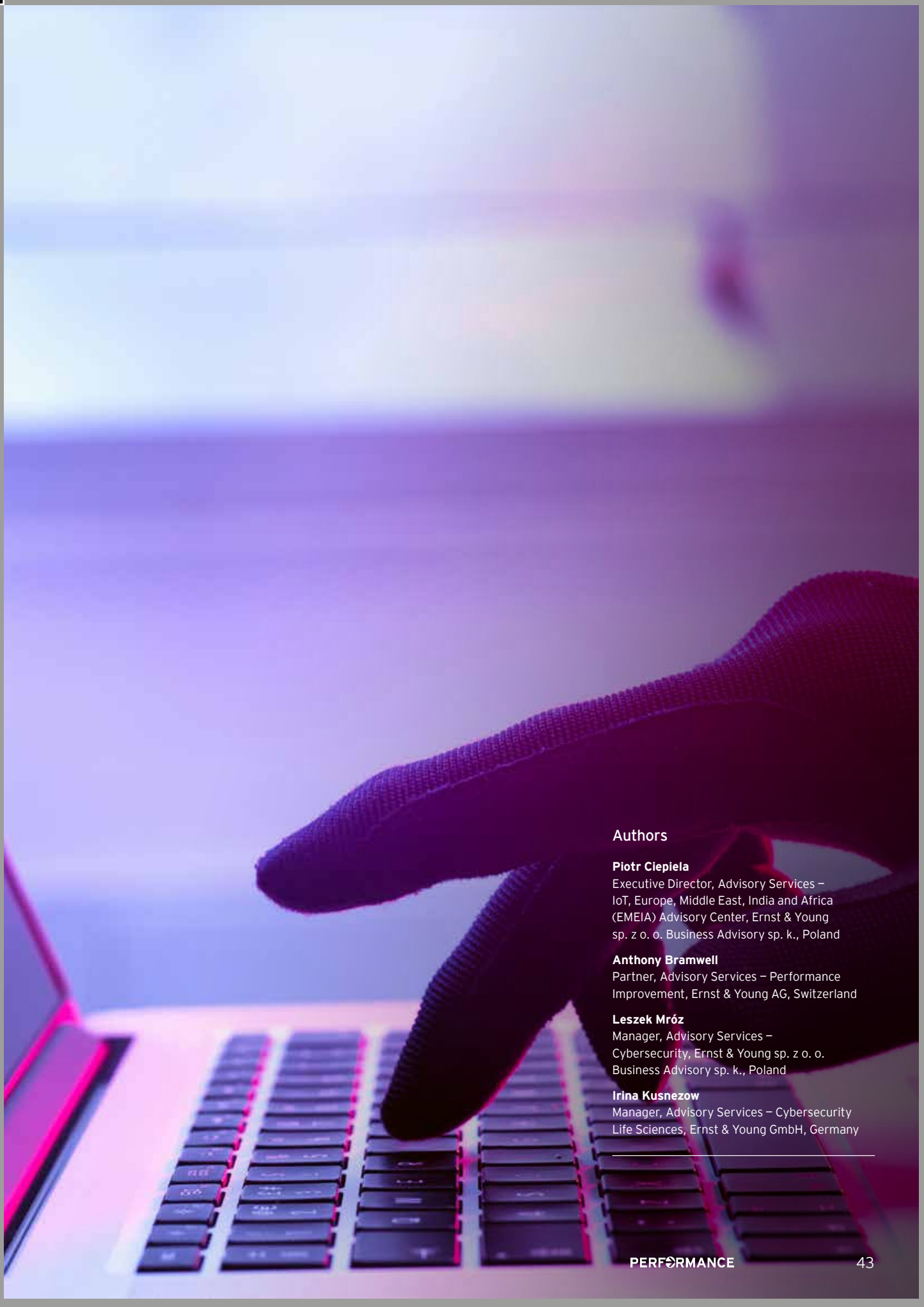
This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

Operational technology security and safety in life sciences

Cybersecurity is a major threat to organizations of all kinds. But until recently, relatively few life science companies have considered the potential risk of attacks on their production and manufacturing environments. Yet there are serious vulnerabilities, for reasons including the expansion of connectivity in these environments or the use of legacy operating systems. Life sciences organizations need to act now to protect themselves and gain competitive advantage in their market.

This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**



Authors

Piotr Ciepiela
Executive Director, Advisory Services – IoT, Europe, Middle East, India and Africa (EMEIA) Advisory Center, Ernst & Young sp. z o. o. Business Advisory sp. k., Poland

Anthony Bramwell
Partner, Advisory Services – Performance Improvement, Ernst & Young AG, Switzerland

Leszek Mróz
Manager, Advisory Services – Cybersecurity, Ernst & Young sp. z o. o. Business Advisory sp. k., Poland

Irina Kusnezow
Manager, Advisory Services – Cybersecurity Life Sciences, Ernst & Young GmbH, Germany

This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

As OT security becomes a widely discussed topic, the awareness of OT operators is rising, but so is the knowledge and understanding of OT-specific problems and vulnerabilities in the hacker community.

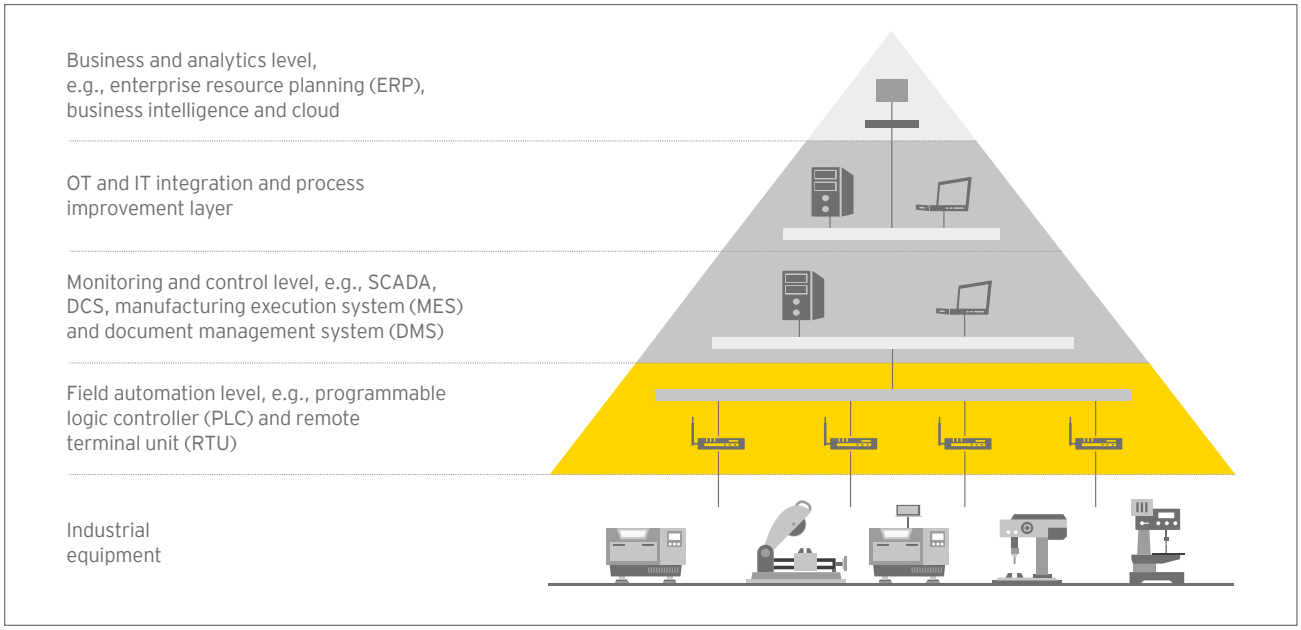
During the last couple of years, the number of cyber attacks on production and manufacturing environments has grown. In particular, shop floor systems, including distributed control systems (DCSs) and supervisory control and data acquisition (SCADA) systems, have become primary targets for attacks.

Many life science organizations have introduced new technology to drive improvements such as production and supply chain efficiency and asset management. This has led to closer and more open integration between IT and shop floor systems — but the increasing connectivity of previously isolated manufacturing systems, together with a reliance on remote supporting services for operational maintenance, has introduced new vulnerabilities for cyber attack. Not only is the number of attacks growing, but so is their sophistication.

As operational technology (OT) security becomes a widely discussed topic, the awareness of OT operators is rising, but so is the knowledge and understanding of OT-specific problems and vulnerabilities in the hacker community.

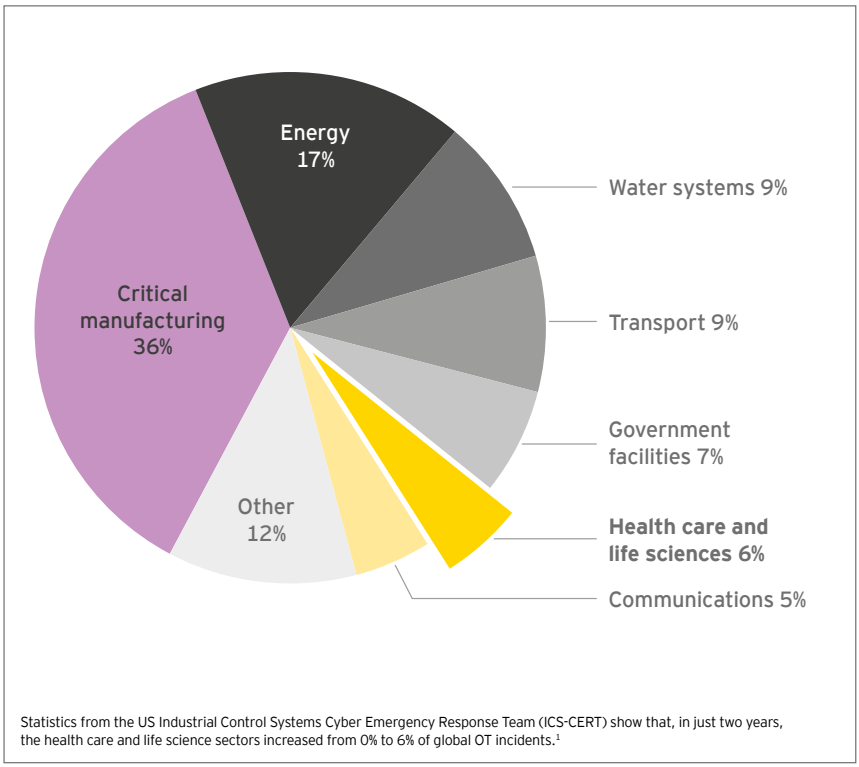
OT environments have very different security requirements, priorities and operational conditions compared with typical corporate IT networks and systems — they are focused on ensuring product quality and the continuity of manufacturing processes. OT system vendors are more eager to utilize proven, reliable technologies than emerging ones, even if they promise improved efficiency, more functionality or scalability; for example, using Windows XP or some older Linux distributions instead of current, patched operating system releases such as Windows 10, or using old, unencrypted Modbus serial protocols.

Figure 1. IT and OT technology pyramid



This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

Figure 2. Share of OT incidents by sectors in 2015



Statistics from the US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) show that, in just two years, the health care and life science sectors increased from 0% to 6% of global OT incidents.[1]

The security aspect alone is very rarely a driver to replace a vendor who is offering the most effective manufacturing equipment.

From the perspective of the organizational units responsible for cybersecurity in life science organizations, OT has been somewhat off the radar. OT systems were treated as an integral part of production machinery rather than computerized information systems, so the ultimate responsibility of its operations, regardless of the cause of potential failure, was assigned to manufacturing maintenance teams. In some examples, only the "technology" aspect was taken into consideration (e.g., protection tools); however, the "people aspects" often seem to be the bigger issue in OT security implementation.

1. "Energy sector tops list of US industries under cyber attack, says Homeland Security report," IoT Now, https://www.iot-now.com/2015/03/12/30962-energy-sector-stays-top-of-the-list-of-us-industries-under-cyber-attack-says-homeland-security-report/, accessed 20 June 2017.

Figure 3. OT security challenges in life sciences

Sophisticated environment

There are a great variety of systems and vendors.

Costs reduction

OT security can be a business enabler rather than another expense.

New legacy systems

Even newly commissioned OT solutions are often still delivered with legacy operating systems.

Specific lab environment

Lab systems are crucial from a quality assurance perspective.

OT governance

Existing security structures rarely cover OT areas that are strictly related to manufacturing.

GxP aspect

There is false assurance that "GxP compliance" means OT security.

This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

In reality, there were no good practices and formal regulations for manufacturers on how to provide even minimal security protection on medical devices.

There are currently some features of OT environments that make them difficult to secure:

1. **Sophistication**

   Manufacturing and lab equipment vendors in the life science sector utilize a great variety of OT technologies and applications. In addition, individual manufacturing facilities have had more autonomy over their choice of systems or facilities, and very different systems have been acquired through mergers and acquisitions.

   This creates a challenge in defining and implementing coherent security policies across production plants. System-dedicated networks, multiple domains and dedicated supporting systems (i.e., engineering tools and backup solutions) require more resources to achieve a maturity level comparable with IT. It also greatly increases the complexity in monitoring and maintaining security levels.

2. **New legacy systems**

   As OT system vendors prefer proven, reliable technologies, at the point of implementation, some OT systems are already only supporting obsolete, insecure operating systems. The security aspect alone is very rarely a driver to replace a vendor who is offering the most effective manufacturing equipment. On the other hand, OT system vendors do not feel obliged to increase the security capabilities of their systems – the technical specifications released by life science organizations at the system acquisition stage rarely include any security requirements at all.

As the risks continue to expand and regulations start to come into place, the time window for competitive advantage through better OT security is closing.

3. **GxP aspect**

   GxP requirements (a set of practice quality guidelines and regulations used in the pharmaceutical industry) cover a significant number of basic security requirements (i.e., related to access control). However, these are focused on only one of three pillars of security — the integrity of generated and processed information.

   Enabling high availability of OT systems and maintaining the confidentiality of some sensitive information processes by those systems require additional security controls. Implementation of an OT security management system requires the alignment of new OT security processes with existing GxP processes — which adds another level of complexity in comparison with other industrial sectors.

4. **IoT revolution and security impact (industrial IoT)**

   The Industry 4.0 revolution is having a great impact on pharmaceutical manufacturing environments. It offers significant opportunities for improving production effectiveness; in particular, based on continual, online information about manufacturing processes and equipment. However, the utilization of new IoT technologies also has an impact on security. New protocols (including wireless) or mesh network architectures increase the number of potential access points to the network and require a different approach to security.

5. **Medical devices**

   More and more incidents related to unprotected medical devices have resulted in the creation of the first security guidelines. For example, in December 2016, the U.S. Food and Drug Administration (FDA) issued *Postmarket Management of Cybersecurity in Medical Devices*,[2] which gives high-level security recommendations.

   But this is just the tip of the iceberg. In reality, there were no good practices and formal regulations for manufacturers on how to provide even minimal security protection on medical devices. As a result, hospitals (and even patients themselves who may have technology fitted in their bodies) are full of vulnerable equipment that has become easier to target — with the potential for direct impact on human lives. Publication of these breaches, and even vulnerabilities, can have a significant impact on company stock prices, with a 2016 example showing a 5% drop in share price following disclosure of vulnerabilities in pacemakers.[3]

Conclusion

The maturity of manufacturing in the life sciences sector is lagging behind other sectors, such as power and utilities or oil and gas, in looking after critical infrastructure.

The advantage of this for life sciences companies is that they can leverage experience from more mature sectors and have access to a number of new vendors and tools in the market, providing technologies to help mitigate some of the key risks. But the challenge all sectors are facing is, of course, the lack of OT security specialists available in the talent pool. Internally, because this issue cuts across manufacturing and IT, the major roadblock is typically obtaining alignment on the organizational reporting lines, responsibilities and, critically, who pays for it.

As the risks continue to expand and regulations start to come into place, the time window for competitive advantage through better OT security is closing. To seize the opportunity for rapid improvements and be successful, it is critical that OT security initiatives are initiated with the strongest possible executive sponsorship. ■

2. *Postmarket Management of Cybersecurity in Medical Devices,* U.S. Food and Drug Administration, 2016, accessed via https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.
3. "Carson Block Takes on St. Jude Medical Claiming Hack Risk," Bloomberg, 25 August 2016, accessed via https://www.bloomberg.com/news/articles/2016-08-25/carson-block-takes-on-st-jude-medical-with-claim-of-hack-risk.