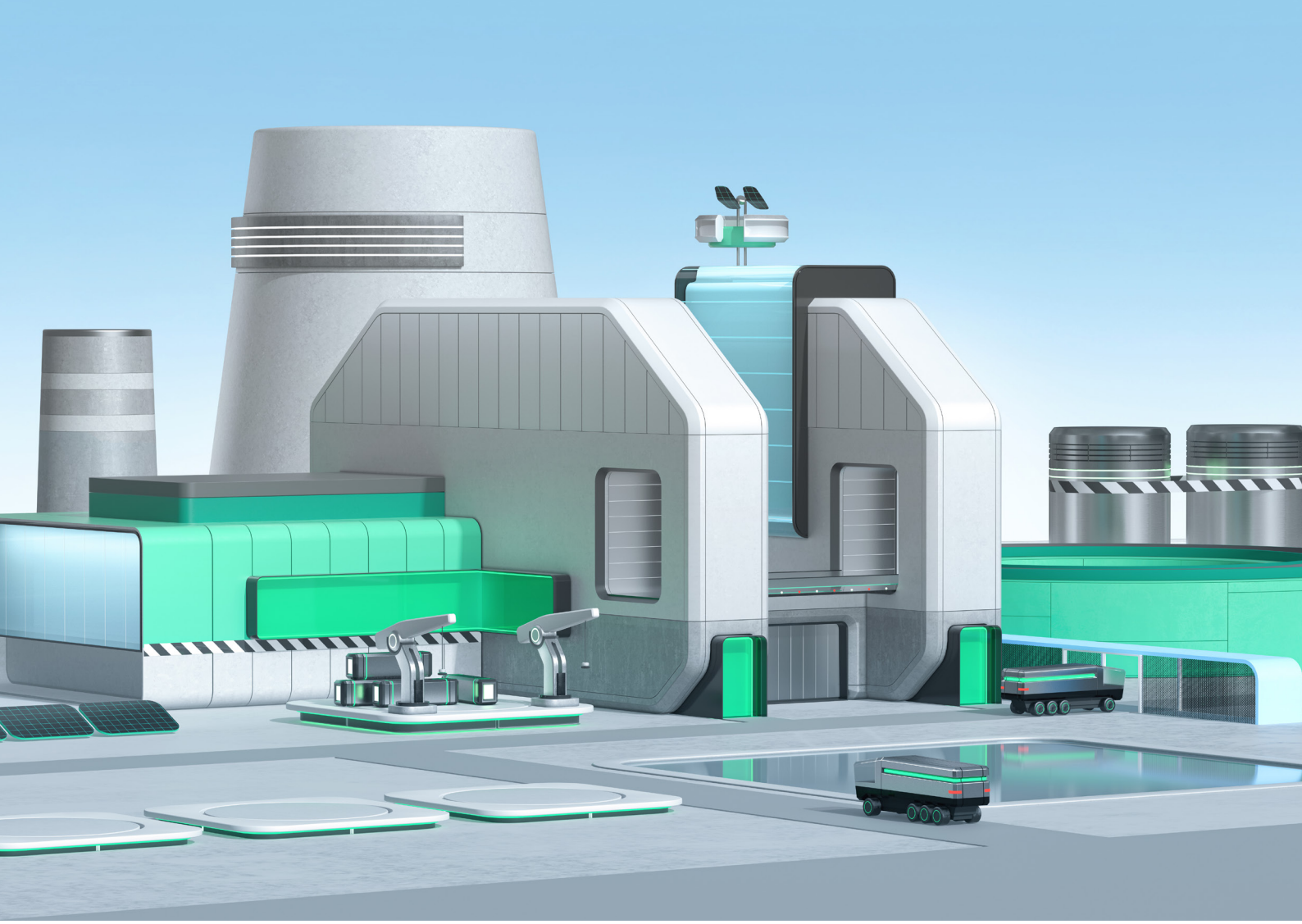


Building a safer future in Heavy Industry

kaspersky BRING ON THE FUTURE

go.kaspersky.com/heavy_industry

2022

Addressing digital challenges of heavy-duty enterprises

All around the world, companies operating in heavy industry, with long histories of building their businesses based on their accumulated expertise in physical plant and equipment, are finding themselves becoming increasingly digital.

They're doing this because digitization helps companies optimize their manufacturing strategies, maximize the efficiency of their facilities and assets, minimize downtime, and simplify compliance with industry regulations.

But as we'll see in this paper, digitization also increases complexity – and, by introducing potential gaps in security, can make industrial operations harder to defend.

If you're in any doubt about the scale of the threat to the security of heavy industry posed by cybercriminals, look no further than the May 2021 attack on the Colonial Pipeline Company, which reportedly shut down 45% of the fuel supply in the Eastern United States.

According to a Bloomberg article, the attack which took down the country's largest fuel pipeline was the result of a single compromised password (one of a batch leaked on the dark web) that enabled hackers to infiltrate the company's networks, even though the account was no longer in use at the time of the attack.

Having gained access to Colonial's networks on April 29, on May 7 the cybercriminals sent a ransom note to the company's control room demanding a cryptocurrency payment, as a result of which Colonial immediately began shutting down the pipeline – the first time the entire system had been shut down in its 57-year history.

The company's pipeline system transports around 2.5 million barrels of fuel daily from the Gulf Coast to the Eastern Seaboard, and news of its shutdown spread rapidly, resulting in queues and higher prices at filling stations, many of which ran out.

Soon after the attack, Colonial began an exhaustive examination of the pipeline, tracking 29,000 miles (47,000 km) on the ground and by air to look for visible damage. Having determined that the pipeline hadn't been damaged and the attackers had not breached its operational technology (OT) systems, Colonial paid a ransom of $4.4 million to the cybercriminals (who had also stolen 100GB of data and threatened to leak it if the ransom wasn't paid) before beginning to resume services on May 12.

What makes an industry 'heavy'?

What exactly does the term 'heavy industry' encompass? There's some discussion about how broad a definition it should be, but in general, and for the purpose of this paper, it refers to the following capital-intensive sectors:

- **Energy – particularly oil and gas, but also coal, electricity, nuclear and renewables**
- **Mining – from precious metals through to steel, copper and other metals and minerals**
- **Shipbuilding, automobiles, aeronautics and other transport**
- **Chemical extraction, manufacturing and development**
- **Any other manufacturing involving heavy machines, equipment or infrastructure**

But while the $4.4 million ransom was considerable, this pales into insignificance compared to the downtime costs for the six days during which the pipeline had to be shut down, not to mention those of ensuring it and the company's other systems were ready to be brought back online, and the damage to Colonial's reputation following the attack.

A compromised password, which itself could have been protected by security as simple as two-factor authentication, is one of the most basic vulnerabilities faced by companies operating in heavy industry. There are many other more serious threats that organizations need to be aware of and capable of defending themselves against.

The 2021 Verizon Data Breach Investigations Report, for example, found that social engineering (primarily through phishing to steal credentials) and system intrusion (largely achieved through more complex, multi-step, human-operated ransomware attacks) are the top attack patterns for companies in heavy industry sectors.

Based on a combination of analysis by leading commentators such as EY, Gartner and McKinsey, and our own experiences in working with heavy industry companies around the world, there are five interrelated trends we believe need to be managed securely if organizations are to mitigate these cyber risks, and maximize the benefits enabled by new technology.

These include:

The relentless advance of digitization

IT/OT integration

The Industrial Internet of Things (IIoT)

Supply chain complexity

The role of human actors

We'll now look at each of these trends – including the potential security risks and how these can be managed more effectively.

Trend #1: The relentless advance of digitization

Throughout heavy industry, increasing digitization is helping organizations meet their most important corporate goals – from driving innovation to addressing productivity, safety, and environmental, social and governance (ESG) priorities.

In mining and metals (M&M) for example, a 2021 report by EY noted that 'Digital and innovation have been key tools in helping miners improve productivity. We expect to see even greater use of data science, modeling and scenario planning to enable more agile decision-making around cost.'

In particular, digital priorities for M&M companies identified by EY include process intelligence (data mining) and automation (RPA), business and operations intelligence, digital asset management, decision intelligence (AI, ML), remote/integrated operating centers, new products and platform development (customer portals, agile factories etc.), cloud adoption and digital trust (blockchain).

Similarly, major trends in oil and gas highlighted by Gartner include:

- Accelerating digital innovation is now table stakes for CIOs
- Digital twins drive transparency and automation
- Comprehensive engineering creates intelligent assets
- Reliance on AI becomes more widespread and less visible
- Multiple disruptions yield hybrid reformation of IT operating model

With so much digital innovation already underway or in the pipeline, it would make sense for these investments to be properly secured. But a 2020 EY article poses the question 'Does cyber risk only become a priority once you've been attacked?'

As it explains: 'Cyberthreats are growing at an exponential rate globally, with more than half of energy and resources participants in EY's latest Global Information Security Survey having experienced a significant cybersecurity incident in the last year.

'Today, all mining organizations are digital by default – in an increasingly connected world, the digital landscape is vast, with every asset owned or used by an organization representing another node in the network.

The mining and metals (M&M) sector is returning to growth, but companies face a transformed competitive and operating landscape. The need to improve shareholder returns will drive bold strategies to accelerate productivity, improve margins and better allocate capital to achieve long-term growth. Digital innovation will be a key tool, but the industry must overcome a poor track record of technology implementations. If M&M companies are to survive and thrive in a new energy world, they must embrace digital to optimize productivity from market to mine. Source: EY

To improve outcomes, such as production efficiency, uptime and yield, oil and gas companies are supplementing traditional monitoring and control systems with additional sensors, cloud-based data aggregation platforms, advanced analytics and AI. According to the Gartner 2021 CIO Survey, as many as 50% of oil and gas companies plan to increase investments in analytics, AI/machine learning (ML), automation, IoT and cloud this year.

AI/ML are quickly gaining acceptance in the oil and gas industry. Gartner survey data suggests that oil and gas CIOs list AI/ML/analytics and the industrial IoT as the top game-changing technologies in 2021. Source: Gartner

'Organizations are increasingly reliant on technology, automation and operations data to drive productivity gains, margin improvement and cost containment goals. At the same time, it has never been more difficult for organizations to understand and secure the digital environment in which they operate, or their interactions with it.'

How to manage digitization securely

Cyber-incidents can be malicious or unintentional. They range from business service interruptions, large-scale data breaches of commercial, personal and customer information, to cyber fraud and ransomware (such as WannaCry and NotPetya) and advanced persistent threat campaigns on strategic targets. Source: EY

US government warnings during 2020 and 2021 highlighted the most dangerous cyberattacks threatening heavy industry. In July 2020, the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint alert in response to a growing number of attacks leveraging spear phishing and ransomware to target industrial networks. NSA followed up in April 2021 with a second cybersecurity advisory on the risks of connecting industrial networks to IT networks. And, following the attack on Colonial Pipeline and other government alerts with respect to ransomware attacks, in July 2021 the White House issued a National Security Memorandum on improving cybersecurity for critical infrastructure control systems.

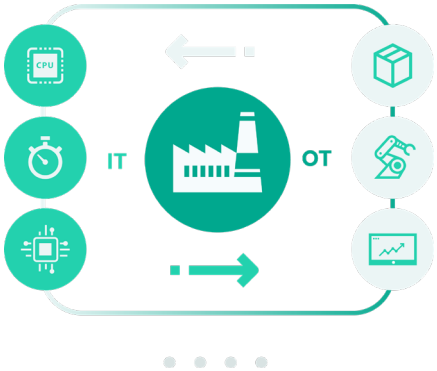
As an example of the task faced by IT security teams working in heavy industry, an article based on the results of EY's Global Information Security Survey 2021 looks at how oil and gas security leaders can smooth the transformation path, but also the challenges faced by CISOs in this rapidly evolving sector.

- Just **29%** of oil and gas cybersecurity leaders say the board or executive management committee understands the value of cybersecurity to the business – noticeably lower than in other sectors.
- Moreover, **6 in 10** warn that the board makes decisions on cybersecurity without having the technical knowledge to understand the threat fully. And oil and gas cybersecurity leaders are also more likely to say that, when they try to make a case for increased funding, the board has trouble understanding why more investment is required.
- Executives have good reason for worrying about the security of their technology systems, as a single security flaw gives hackers **an opportunity to bring down a whole network**. So it is concerning that many oil and gas companies are investing in technology without ensuring they have built in the appropriate security resilience, with fewer than half **(48%)** of respondents saying they are brought in at either the planning or design stage of a new business initiative.
- This is further complicated by the fact that a significant percentage of business expansion relies on large turnkey third-party engineering contracts, where the ownership of the risk is at times unclear and lacks accountability.
- More than **6 in 10 (65%)** oil and gas respondents admit the business rolls out new technology to timescales that do not allow time for suitable assessment. They also flag that the most challenging aspect of their role is supporting new technology-driven initiatives.

As we saw in the introduction to this paper, it only takes a leaked password for a business to be exposed to millions of dollars in potential damage. But breaches can also result from everything from unpatched legacy systems to human error or deliberate fraud. It's vital, therefore, that companies operating in heavy industry take note of these kinds of issues, and implement appropriate cybersecurity to mitigate the threats to which they're increasingly being exposed.

Endpoints – including servers, workstations and mobile devices – are the source of the majority of cybersecurity problems encountered by organizations. As a result, high quality endpoint protection has to be the first line of defense against attempted security breaches. And those organizations planning to or already moving applications and/or data to public, private or hybrid cloud environments also need to invest in specialist cybersecurity specifically designed to secure these workloads.

Plus, as heavy industry can be targeted by everything from commodity threats to equipment sabotage and nation-state attacks, it's vital for organizations to develop a clear understanding of the cyberthreat landscape confronting them, and implement appropriate security measures – such as more advanced endpoint detection and response solutions, specialist threat intelligence and cybersecurity services – capable of anticipating and effectively mitigating these threats.



Trend #2: IT/OT integration

In order to maximize the benefits of digitization, heavy industry companies face the complex task of integrating two very different environments: their traditional operational technology (OT) world of physical machines, electromechanical devices and other industrial equipment; and the virtual (IT) world of servers, storage, networks and other devices needed to host and run applications and process data.

Until recently, these two worlds were almost completely separate, sharing very little (if any) data or control, and being operated by teams and personnel with completely different skillsets. Unsurprisingly, merging the two worlds' business processes, insights and controls into a single integrated IT/OT environment is proving far from trivial. And this in turn is opening new security gaps.

As EY has pointed out, 'Historically, OT environments were isolated, with limited connectivity to external networks beyond the physical site, and utilized vendor-specific protocols and proprietary technologies.

'This often allowed asset owners to adopt a "security by obscurity" approach. However, this approach is no longer viable within modern OT environments as they are highly connected and increasingly leverage infrastructure, protocols and operating systems that are also common within enterprise IT. As such, vulnerabilities associated with technologies utilized within enterprise IT are often equally applicable for critical OT.'

With increasing investment in digital, reliance on automation systems, remote monitoring of infrastructure for long-term cost efficiency and near real-time decision-making across the value chain, it is the norm for mining and metals companies to have thousands of OT devices connected across geographical environments.

However, the increased connectivity of these devices, and by extension the increased attack surface, means that the physical security of remote mining and metals operations is no longer sufficient. Additionally, equipment and infrastructure that have traditionally been disconnected (e.g., autonomous drills, trucks and trains) are now integrated to provide greater control of operations.

This combination of events, coupled with system complexity and third-party risks, have led to a further expansion of the "attack paths" that may be used in cyber-incidents. Hackers who exploit these paths frequently utilize a number of common weaknesses found within network architecture, legacy industrial technologies, basic access controls and security configurations, maintenance processes, remote staff and third-party access, and security awareness.

As a result, the entire supply chain is now at risk, which is not limited to the potential of causing disruptions to operations, but worse, significant health and safety consequences (e.g., resulting from shutdown or overriding of fail-safe systems, physical failure of infrastructure, equipment operating outside of expected parameters etc.). If these risks are not being effectively identified, tracked and monitored, it is likely that the organization and its employees will be left significantly exposed.
Source: EY

A major issue arising from this is that many of the security tools and approaches used by heavy industry simply aren't keeping up. To take one example, most of today's OT networks consist of legacy equipment originally designed to be safeguarded from unsecured networks by perimeter protection such as firewalls. Yet firewalls offer little or no protection against attacks (such as malware on removable devices) originating within the OT network itself.

Similarly, many traditional security tools cannot be applied to an OT environment; can actually harm the devices that control plant equipment; and even using them for scanning can cause major plant disruption.

Applying security patches to address known vulnerabilities presents further risks, as few sites have representative backup systems on which to test the patches. And many OT environments continue to use versions of Windows for which Microsoft no longer provides security patches – creating built-in vulnerabilities for the systems involved.

Because they need to support specific requirements, OT environments are often also highly customized 'black boxes', making their precise operation difficult for users to understand – let alone how to protect them. This is why companies tend to rely on original equipment manufacturers (OEMs) or third parties for maintenance and upgrades. But cybersecurity reviews are rarely included in OEM contracts, security standards are rarely enforced, and OEM vendors report that operational buyers rarely want or use security features, even if they're built in.

New technologies such as cloud services, wireless networking and mobile industrial devices are adding to this complexity – and the associated risks. And the global shortage of cybersecurity professionals is also a

particular problem for heavy industry companies needing to protect both IT and OT systems, as they may find it very difficult to recruit the right people.

These issues affect not just current procedures and controls, but also the implementation of new tools and ways of working. And the drive to integrate IT and OT environments is taking all of them to a whole new level.

How to manage IT/OT integration securely

As companies undergo digital transformation, leaders are integrating cybersecurity earlier, in both the OT and IT environments. If heavy industrials are to manage risk and avoid security-driven delays during their digital transformations, they will need to embed security earlier in the process, with investments in developer training and oversight. At the same time, these companies should expect increased convergence between their OT and IT systems. Therefore, their investments in cybersecurity transformation programs should span both, while they more deeply integrate their security functions into both the OT and IT ecosystems.

One way to accomplish this is to create an integrated security operations center that covers both OT and IT, housing detailed escalation protocols and incident response plans for OT-related attack scenarios. Solutions like these enable centralized asset management, security monitoring and compliance, dynamically and in real time.
Source: McKinsey

Organizations need to apply good risk management principles, and this starts with thinking about issues such as cyber risk in the same way as any other business risk.

Understanding the cyberthreat landscape is a vital foundation step in improving cyber maturity, and developing a clear plan that forms part of an organization's digital roadmap and risk management plan.

The first step is to establish a baseline of basic cyber controls. This, supported by a risk-based approach to prioritizing strategic and long-term cyber investment, should be aligned with the organization's top cyberthreat scenarios.

To enable this, organizations should adopt a cybersecurity framework for the consistent identification of critical cyber control gaps, threats and actions required to achieve the target risk profile. This includes:

- **Identify the real risks:** Map out critical assets across systems and businesses
- **Prioritize what matters most:** Assume breaches will occur and improve controls and processes to identify, protect, detect, respond and recover from attacks
- **Govern and monitor performance:** Regularly assess performance and residual risk position
- **Optimize investments:** Accept manageable risks where budget is not available
- **Enable business performance:** Make security everyone's responsibility

Trend #3: The Industrial Internet of Things (IIoT)

If you're not already engaged in pilot projects assessing the benefits of the Industrial Internet of Things (IIoT) or actively using the technology to improve your operations, you soon will be.

The IIoT is an industrial framework through which large numbers of machines and/or devices, ranging from complex industrial robots and machine tools to tiny environmental sensors, are connected and synchronized.

Most IIoT devices are sensors used to monitor manufacturing and industrial processes, with data from the various types of sensors being transmitted to monitoring applications that ensure key processes are running optimally – for example by minimizing costs and improving reliability, responsiveness, quality and delivery.

Commonly used applications of IIoT include smart metering, smart grids, smart factories and many more. And in heavy industry, IIoT devices such as meters, sensors and alarms are particularly significant, with applications including real-time data analytics and equipment monitoring, location intelligence, predictive maintenance, machine automation, and personnel or third-party monitoring.

In a 2021 report, McKinsey states that 'It has been technologically possible to implement IIoT-based use cases for a couple of years already. What we are witnessing now, however, is the opening up of completely new possibilities for implementing sophisticated, innovative use cases in a streamlined way. What's more, plants in the World Economic Forum's Global Lighthouse Network are demonstrating leading-edge capabilities. If done right, leveraging an IIoT-enabled backbone can lead to game-changing improvements in the performance (metrics) of manufacturing companies - across industries and with a wide range of use cases.'

$500 billion

IIoT will be a $500 billion market by 2025 as advances in its essential technologies drive up demand.
Source: McKinsey

How to manage IIoT securely

According to a study by Forrester Consulting:

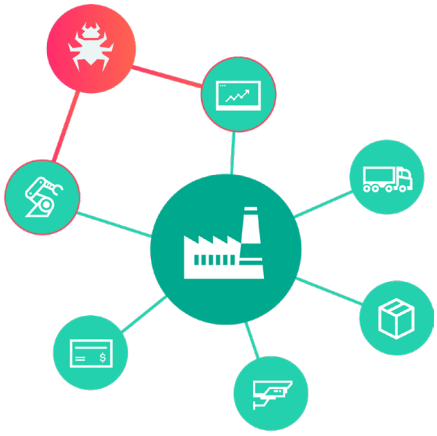
- **73%** of organizations surveyed estimate that at least half of all devices in their enterprise are unmanaged or IoT devices
- **74%** are 'very-to-extremely concerned' about the risks posed by unmanaged and IoT devices
- **66%** have experienced an IoT-related security incident
- **96%** plan to increase their budget dedicated to unmanaged and IoT device security

Source: Armis

As connected devices become increasingly integral to industrial processes, the security risks associated with them can be difficult to understand and mitigate.

Connected devices face the risks of being a part of the corporate network, as well as those unique to the embedded systems on which they're based. Traditional antivirus solutions, however, cannot fully defend against the latest advanced, targeted and malware threats to embedded systems, which therefore require specially designed, multi-layered intelligent protection based on a combination of Default Deny with Device Control.

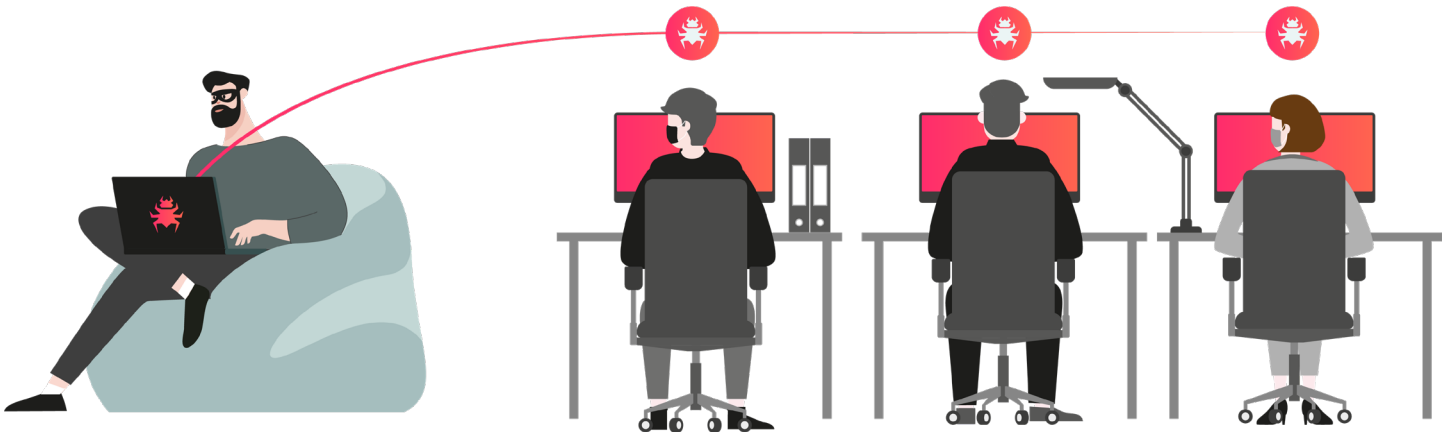
In tandem with this, the poor security of the majority of IoT devices creates its own threats. These require the implementation of specialist security across the IoT/IIoT ecosystem – minimizing risk and addressing cybersecurity threats to IoT systems and embedded devices through tools securing every software and hardware component of these interconnected systems – without overloading individual systems or devices or limiting overall flexibility.



Trend #4: Supply chain complexity

Cyberthreats targeting multiple groups at once are among today's most widespread and effective attacks. The 2020 SolarWinds attack, for example, which infected a trusted software update used by many well-known companies, provided a glimpse into the potential dangers of supply chain attacks. These interrupt one link within an organization's supply process to cause massive disruption – with vulnerable endpoints enabling hackers to gain access to major companies via their partners and suppliers.

For heavy industry, their scale of operations, geographical spread, and the critical infrastructure they represent, make organizations attractive to anyone wanting to make a big statement or achieve a massive impact, while their complex supply chains make them especially vulnerable to cyberthreats such as phishing and ransomware.



A long supply chain of many interconnected companies provides a perfect channel for phishing attacks involving carefully crafted, official-looking emails that appear to originate from an organization with which the company already does (or might wish to do) business. Often, these emails also include readily available details of an executive or colleague the hacker wishes to impersonate.

All a recipient has to do is click on an attachment or malicious link, and they'll have provided the cybercriminal with a discreet entry point into the organization's network which can then be used to gain all the information needed to mount a full-scale attack.

Similarly, for ransomware, a vast network of OT devices throughout a long supply chain provides multiple endpoint vulnerabilities, while fragmented systems leave numerous security gaps.

As we've already seen from the Colonial example, cybercriminals can wreak havoc through attacks that encrypt or freeze access to a company's systems and networks, and/or threaten to leak confidential data. And in industries where time (and particularly downtime) translates directly into hard cash, it's often more cost-effective to pay a ransom than waste time and resources attempting to recover from the attack.

With long supply chains depending on parts or products, ransomware can also have much broader implications, with other companies and industries becoming affected by the disruption within days. This impact can be even more damaging to the original victim, as business relationships are lost and customers learn of the breach.

How to manage supply chain complexity securely

While it's unrealistic to expect organizations to police the cybersecurity of their extended supply chains, as we've seen throughout this paper, there are a variety of steps they can take to harden their defenses against the kinds of attacks that use the supply chain as a means of access to corporate systems.

Phishing, for example, generally requires an employee to open a malicious attachment or click on a malicious link. And, sophisticated as many phishing emails have become, there are often telltale signs that they haven't originated from where they appear to, which can be addressed through improved security awareness.

Ransomware, meanwhile, has no place in society, which is why we're so determined to eradicate it – both through Kaspersky products and our participation in initiatives such as No More Ransom. This free online resource offers advice on ransomware prevention, and answers to questions on a range of topics including different types of ransomware, whether or not to pay a ransom, how to decrypt files encrypted by ransomware and more.

For organizations unfortunate enough to have suffered an attack, the site also provides a Crypto Sheriff to identify the specific type of ransomware affecting a device, and whether one of the hundreds of free tools available on the site is able to decrypt it.

Trend #5: The role of human actors

Security efforts in heavy industry have often focused on the network perimeter and implementing measures to block external threats, but insider threats can be just as damaging if not more so.

Insiders can steal sensitive information for financial gain, take information to provide to their next employer, or abuse their privileged access to cause significant harm. Insider breaches can also have major consequences for organizations, including reputational damage, loss of revenue, the theft of intellectual property, reduced market share and even physical harm.

Reflecting the scale of the threat posed by insiders including current and former employees, contractors, or other individuals with inside knowledge about an organization, in October 2021 the US Government's Cybersecurity and Infrastructure Security Agency introduced a new Insider Threat Risk Mitigation Self-Assessment Tool to help public and private sector organizations further their understanding of insider threats and develop prevention and mitigation programs.

While large organizations are likely to have conducted risk assessments and put measures in place to mitigate insider threats, small and medium-sized businesses tend to have limited resources and may not have assessed their risk level. The tool therefore consists of a series of questions to establish the level of vulnerability to insider threats, and provide feedback to help users develop appropriate mitigations to guard against insider threats and reduce risk to a low and acceptable level.

How to manage insider threats securely

Effective cybersecurity mandates removing practices that are inherently risky, such as:

- Continued use of software that has reached its end-of-life and is no longer supported by the software developer – as without support, patches are no longer issued to correct vulnerabilities, which can be easily exploited by cyber actors to gain access to internal networks.
- Failure to change default credentials and passwords that are known to have been compromised in data breaches or have otherwise been disclosed.
- Using single factor authentication for remote or administrative access to systems – which, while this provides a degree of security, it is not sufficient to resist the brute force tactics of hackers.

To reduce the risks posed by insider threats, putting policies in place to immediately prevent access to corporate systems by former employees should unquestionably be added to this list. And, given that in any environment people can still make honest mistakes, interactive and compelling cybersecurity awareness training that helps to reduce these errors is another vital investment.

Summary

Although the term 'heavy industry' covers organizations engaged in widely differing activities and sectors facing diverse challenges, as we've seen in this paper, when it comes to technology, many are being forced to deal with broadly similar trends. Digitization, IT/OT integration and IIoT adoption are accelerating, supply chains will only get more complex, and internal threats will not go away. But as it stands, in terms of cybersecurity, heavy industry simply isn't keeping up – which means headline-grabbing attacks such as the one on Colonial Pipeline will become more common, not less so.

Kaspersky is a pioneer in helping heavy industry companies protect data and business continuity 24/7 against cyberthreats ranging from commodity, advanced and evasive threats to targeted attacks – mitigating risks, detecting attacks earlier, dealing effectively with live attacks and fortifying future protection.

Our **stage-by-stage** cybersecurity approach is designed to clarify which level of security as well as which specific solutions best suit your organization. The stages provide a set of easily managed threat protection measures coordinating seamlessly with one another to meet the needs of each individual organization, and offer a cybersecurity roadmap assuring a smooth transition from one IT security maturity level to another when the time comes.

Kaspersky's step-by-step cybersecurity approach

1

Kaspersky Security Foundations — essential core of cloud-based, automated protection for all devices, VDI and hybrid server infrastructures, before organizations advance seamlessly to ...

2

Kaspersky Optimum Security — for organizations requiring more specialized security against new and evasive threats, before effortlessly implementing ...

3

Kaspersky Expert Security — for organizations with established mature IT security teams combatting the most complex targeted attacks.

Cybersecurity maturity level	Solution
IT Smaller organizations without a specialized IT security team	**What** Kaspersky Security Foundations **How** Implement fundamental security for organizations of any size and infrastructure complexity, delivering cloud-managed automatic prevention of commodity cyberthreats on any devices, VDI and hybrid server infrastructures. ▪ **Endpoints:** Protect every endpoint in your organization with Kaspersky Endpoint Security for Business; Kaspersky Embedded Systems Security ▪ **Cloud:** Benefit from borderless security with Kaspersky Hybrid Cloud Security ▪ **Network:** Secure your perimeter with Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway ▪ **Data:** Safeguard valuable and sensitive data with Kaspersky Security for Storage ▪ **Security Management:** Access expertise with Kaspersky Premium Support; Kaspersky Professional Services
IT security Organizations in need of advanced defenses, but with limited specialist IT security resources	**What** **Kaspersky Optimum Security** **How** Combat evasive threats with effective endpoint detection and response and continuous security monitoring – but without prohibitive costs or complexity ▪ **Advanced detection:** Boost ML behavior analysis, sandboxing, threat intelligence and automated threat hunting* with Kaspersky Sandbox, Kaspersky Threat Intelligence Portal and Kaspersky Managed Detection and Response Optimum ▪ **Analysis and investigation:** Enhance threat visibility and simplified investigation process with Kaspersky Endpoint Detection and Response Optimum ▪ **Rapid response:** Deploy automated in-product response options, as well as guided and managed response scenarios* with Kaspersky Endpoint Detection and Response Optimum **and** Kaspersky Managed Detection and Response Optimum ▪ **Security awareness:** Equip employees with automated tools at all levels and develop key cybersecurity skills with Kaspersky Security Awareness Training *Supported by Kaspersky experts

Mature and fully formed IT security team and/or dedicated SOC

- Have a complex and distributed IT environment
- Are a highly likely target for complex and APT-like attacks
- Have a low risk appetite due to high costs of security incidents and data breaches
- Are concerned about regulatory compliance

What

Kaspersky Expert Security

How

Complete mastery over the most complex and targeted cyberattacks

- **Equipped:** Equip your in-house experts to address complex cybersecurity incidents. Benefit from a unified cybersecurity solution. Kaspersky Anti Targeted Attack Platform with Kaspersky EDR at its core empowers your team with XDR capabilities.

- **Informed:** Enrich your knowledge pool with threat intelligence and upskill your experts to deal with complex incidents:
  - Integrate actionable, immediate threat intelligence into your security program. Kaspersky Threat Intelligence gives you instant access to technical, tactical, operational and strategic threat Intelligence.
  - Develop your in-house team's practical skills, including working with digital evidence, analyzing and detecting malicious software, and adopting best practices for incident response, with Kaspersky Cybersecurity Training.

- **Reinforced:** Call upon external experts for security assessment, immediate support and back-up:
  - Take advantage of immediate support from the Kaspersky Incident Response team of highly experienced analysts and investigators to fully resolve your cyber-incident, fast and effectively.
  - Bring in a second opinion and managed threat hunting expertise from a trusted partner with Kaspersky Managed Detection and Response, so your in-house IT security experts have more time to spend reacting to the critical outcomes requiring their attention.
  - Understand just how effective your defenses would really be against potential cyberthreats, and whether you're already the unwitting target of a long-term stealth attack, through Kaspersky Security Assessment.

Targeted Solutions

What	How
 **Kaspersky Industrial CyberSecurity**	KICS offers a holistic approach to industrial cybersecurity, bringing value to any stage of your OT security process – from cybersecurity assessments and training to advanced technologies and incident response. An ecosystem of integrated products and services enables you to secure operational technology layers and elements of your organization — including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers — without impacting on operational continuity and the consistency of industrial process.
 **Kaspersky ISC Security Assessment**	For organizations concerned about the potential operational impact of IT/OT security, Kaspersky provides a minimally invasive pre-installation cybersecurity assessment. A crucial first step in establishing security requirements within the context of operational needs, this can also provide significant insight into cybersecurity levels without any further deployment of protection technologies.

Cyberthreats News: www.securelist.com
IT Security News: www.kaspersky.com/blog
Threat Intelligence Portal: opentip.kaspersky.com
Technologies at a glance: www.kaspersky.com/TechnoWiki
Awards and recognitions: media.kaspersky.com/en/awards
Interactive Portfolio Tool: kaspersky.com/int_portfolio

kaspersky BRING ON THE FUTURE