Deloitte.

# Stepping into the Future of Cyber

**Energy, Resources & Industrials**

Deloitte's *2023 Global Future of Cyber Survey* reveals that cyber increasingly plays a foundational role in delivering business outcomes. For energy, resources, and industrial (ER&I) organizations, the quality of those outcomes will depend on how well decision-makers secure their business through a strategic "zero trust" approach as their connected system landscapes grow.

## What does the future of cyber look like for the industry?

**These five highlights provide a glimpse into where energy, resources, and industrial organizations are now—and where they are going.**

### Investing

**59%**

of ER&I respondents say their company's annual cyber spend will increase next fiscal year

### Talent

**59%**

of ER&I respondents say training and certification programs is the top strategy to engage, retain and develop existing talent

### Priorities

**51%**

of ER&I respondents say that cloud, data analytics and AI are the top three digital transformation priorities in the next three years

### Opportunity

**43%**

of ER&I respondents say that cyber plays a crucial role in new or upgrades to operational technologies

### Stability

**36%**

of ER&I respondents say that adoption of emerging technologies will improve operational stability - including supply chain and partner ecosystems

# Becoming cyber-ready

**How can energy, resources, and industrial organizations prepare for an evolving cyber landscape? The following five insights and corresponding actions, based on Deloitte's experience and our survey findings, can provide a starting point for navigating the future of cyber.**

| Insights to inspire | Actions to consider |
|---|---|
| 1. **Spending realities are sinking in.** Across the C-suite and boardrooms, leaders are coming to the realization that cyber spending cannot be a one-time or short-term investment. It should be a steady annual commitment, though the exact spending range may flex from year to year. Emerging cyber regulation can remove management discretion and create tension in use of funds (e.g., compliance vs. risk reduction). | **Know your number.** Cyber is a constant need. Develop a consistent annual spending baseline—to address essential needs and support ongoing innovation. It can help you embed cyber continuously across your business and manage stakeholder expectations. |
| 2. **Cyber talent is becoming scarce.** Skilled cyber specialists are in high demand, and many will gravitate toward employers in industries they perceive as more attractive or sustainable. Our survey data shows that training and certification programs are the number one strategy within ER&I. Organizations should continue to expect increased difficulty attracting and retaining talent. | **Put AI to work for your organization.** Artificial intelligence can provide a strategic solution for talent shortages. Supplement AI by considering which services to source in-house and which to outsource. These options can assist with proactive identification and action of cyber issues, including threats. |
| 3. **Digitalization is big and getting bigger** Industry has made great strides in digitalization, and survey data shows cloud, AI, and data analytics among top transformation priorities. There is growing interest in emerging technologies, including quantum, blockchain, and digital twin. Meanwhile, privatized critical infrastructure assets come with massive technical debt and no guarantees for funding of updated cyber controls. | **Bring together OT, IT, and cyber planners early and often.** As OT and IT continue to converge from an IT perspective, cyber becomes more critical. Do not let it be an afterthought. As you make infrastructure plans, ensure that cyber leaders are part of the conversation from the beginning. |
| 4. **The intersection of OT and IT is still a key improvement opportunity.** While many ER&I organizations have bolstered security for their operational technologies—and how they connect with IT and digital processes—cyber breaches consistently affect OT systems and processes. Organizations of all sizes realize that security is integral to creating products and that they have more work to do. | **Be more strategic about your suppliers.** Cyberattacks are part of modern society, and the reach has expanded to include critical businesses—making supplier reliability a top concern. As the network of potential suppliers change, understand their cyber posture. |
| 5. **Securing the supply chain offers a business advantage.** Physical and software supply chains are increasingly dependent on digitalization, the integrity of the nth parties, and the ability to manage cyber risk—often the result of market events, natural disasters, or regional conflict, as well as cyberattacks. Organizations that make supply chains more cyber-secure gain an edge for their suppliers, customers, and internal processes, reducing and easing stakeholders' concerns. | **Know how you will measure cyber impact.** Our survey reveals that, as a whole, the ER&I industry is slightly ahead of other industries on cyber planning and activities. Make a realistic and true evaluation of your organization's posture. Identify the data, KPIs, and results you need to be truly cyber-confident. |

To get a broader view of the cyber landscape, explore additional insights from the *Deloitte 2023 Global Future of Cyber Survey*, which asked 1,110 leaders across industries and across the globe to share their views on cyber threats, enterprise activities, and the future.

Deloitte.

www.deloitte.com/futureofcyber



Energy, Resources & Industrials