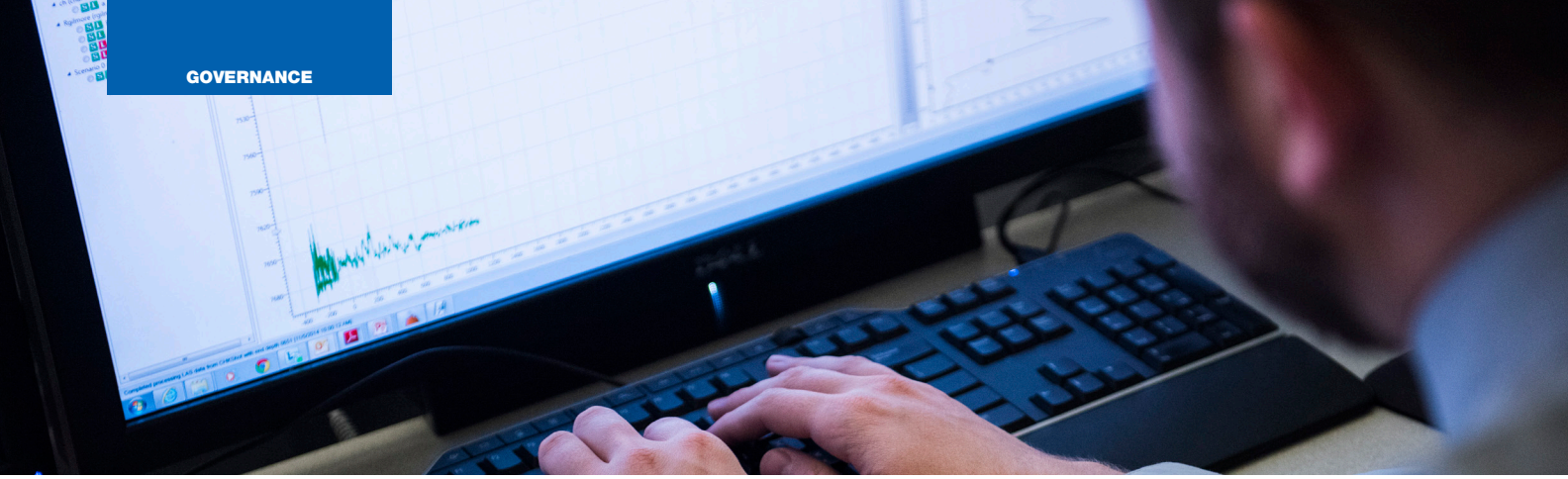

Cybersecurity:
Protecting Our Data, Securing Our Operations

Oil and natural gas companies like Chesapeake use sophisticated technology to power many of the functions central to our industry. While advanced technology provides immeasurable value to our operations, it can also create risk. Specifically, as our business has become more dependent on digital technologies, those same digital capabilities generate opportunities for cyberattacks, exploiting internal or third-party vulnerabilities.

To counteract these threats, we've developed a comprehensive defense approach. Recognizing that no single defense technology alone will be effective in mitigating all cyber risk, our Cybersecurity team utilizes an extensive framework of controls that detect, identify and protect against or mitigate potential cyberattacks.

Cybersecurity Protection Layers

Network and Application Security	Data Protection	Risk and Compliance
Protecting company networks and applications from attack and inappropriate access	Preventing data breaches through a number of security layers	Managed as an enterprise risk, accountable to top company leadership
Identity	**Incident Response and Business Recovery**	**Cybersecurity Awareness**
Protecting the attributes of individual digital identities	Cohesive planning to respond quickly and minimize impact	Training for employees and contractors to prevent unintentional cyber risk

The Cybersecurity team also develops response and recovery plans should an incident occur. This program closely aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework to best protect the data and programs critical to our business. We audit a portion of our information security program every year, using a third-party organization to review our cybersecurity posture from an external perspective.

Increasing Cybersecurity Awareness

As we continue to study and plan for evolving cyber risks, Chesapeake equips our first line of defense — Chesapeake employees — with up-to-date trainings and information. Through targeted communications, annual trainings and cyber exercises, we work to raise cybersecurity awareness among our employees and partners, reminding them of the critical role they play in protecting our digital assets.

We had no major cybersecurity breach or system compromise during 2021.

While employees are often at the front lines of our defense, cybersecurity accountability reaches to the very top of our organization. Our Cybersecurity team provides regular updates to Chesapeake's senior leadership and our Board's Audit Committee about cyber threats, potential vulnerabilities and the proactive security programs in place to protect our operations.

Even with comprehensive protection measures in place, we must continue to strengthen our digital defenses. Information technology is a rapidly evolving field with constantly changing threats — a reality that pushes us every day to prevent, protect and be proactive for the security of our assets and the welfare of our employees.