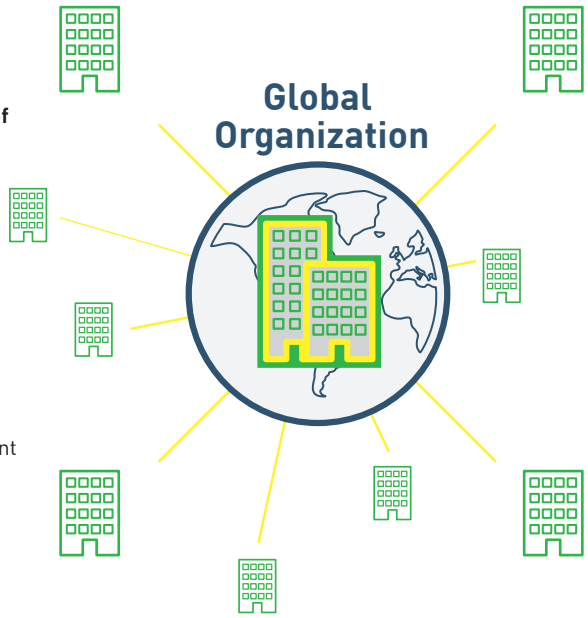
FORCEPOINT

WORKFORCE MONITORING

Laws and regulations differ around the globe...

United States

Employee monitoring activities are governed by a range of federal and state laws providing protections for electronic communications. The **Federal Cybersecurity Information Sharing Act of 2015** ("CISA") provides a broad immunity for employee monitoring activities undertaken for cybersecurity purposes.



Germany

If employers prohibit all personal use of electronic communications tools or allow personal use only and if employees consent to monitoring, employers may engage in reasonable monitoring of the use of electronic communications resources, including Internet access. Otherwise, according to German data protection authorities, **the Telecommunications Act** generally prohibits employers from monitoring the contents of communications absent employee consent.

United Kingdom

If monitoring tools do not capture personal data, the tools are not subject to the restrictions of data protection law. Monitoring that involves the interception of communications during transmission is governed by the **Regulation of Investigatory Powers Act.** Such access is permitted if both the sender and recipient consent, or if the access involves analyzing business-related communications for the purpose of monitoring compliance with United Kingdom laws and regulations or reasonable internal policies.

Singapore

Personal Data Protection Act 2012. Although consent is generally required for the collection, use and disclosure of personal data, employers may process personal data without consent to support monitoring programs - if such processing reasonably supports the management or termination of employment relationships, including as necessary to evaluate the suitability, eligibility, or qualifications of an employee for promotion or continued employment.

Multiple business stakeholders are involved...

HR

A workforce monitoring program can provide real benefits for HR in terms of understanding risk and protecting employees. HR must engage as gatekeeper, designer and advocate of an effective and employee-centered cyber defense program. They must promote transparency and proportionality in the program to maintain the trust of employees, whose support is vital to the success of the program. HR must be included in the development of workforce monitoring programs because the programs will have a human impact.

Legal

Globally, workforce relationships are governed by a range of laws and regulations. Legal plays a vital role to guide on the applicability of such laws and regulations to workforce monitoring programs. In addition, Legal teams should advise on privacy notices and consent mechanisms.

Business Owner

It is important to involve business owners in the development of workforce monitoring programs so they can help identify the critical systems and "crown jewels" that warrant increased protection, clarify what constitutes normal behavior for employees, and support the development of acceptable use policies.

Information Security

Information Security is now a boardroom issue, particularly in light of new regulations such as the General Data Protection Regulation (GDPR). Workforce monitoring governance teams should include representation from Information Security so that risks to information assets are addressed appropriately. Educating Information Security teams about data protection/privacy issues as well as the potential impact of monitoring programs on the workforce will help promote trust, particularly when Information Security teams are called upon to assist with assessments or investigations.

Legal Compliance Effort to Implement Workforce Monitoring Programs

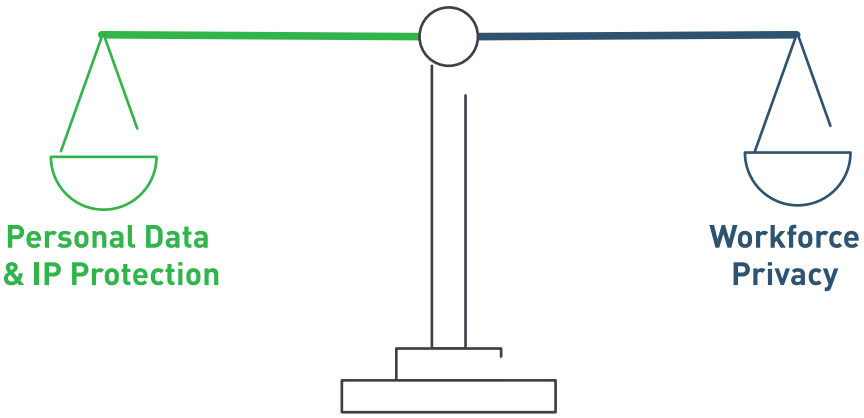
Less effort — More effort

United States, Australia, South Africa, Singapore, Canada, Turkey, Sweden, UK, Netherlands, Spain, Switzerland, France, Germany, Italy, Finland

Approximate characterization of the level of compliance resources required to implement a comprehensive workforce monitoring program for cyber threat management in a particular country.

Finding the Balance...

New laws and regulations, such as the GDPR, require organizations to increase the focus on how they protect and use personal data. And with recent, high-profile data breaches costing organizations millions in lost revenue and shareholder value, there is a need for more advanced, human-centric security programs to protect data.



Human-centric security, by definition, requires behavioural analysis through workforce monitoring. Such programs recognize that workforce members have rights, and the programs work to protect the workforce as well as the organization. A human-centric security program must be deployed proportionately, respectfully, and transparently to promote workforce trust.

In general, there are three areas of law that govern cyber defense programs that involve monitoring of workforce activities: data privacy and data protection laws, communications secrecy laws and employment laws.

Harriet Pearson
Partner
Hogan Lovells

James Denvil
Associate
Hogan Lovells

Protecting the workforce from both inside and external threat is a critical component of a CISOs role today. Protecting the workforce from being the victim or cause of a data breach, whilst preserving privacy, is both a moral and ethical duty of a mature security program.

Allan Alford
CISO
Forcepoint

Hogan Lovells

Managing Workforce Cyber Risk in a Global Landscape: A Legal Review
Read this whitepaper for a review of legal requirements and leading practices, including a review of 10 monitoring use cases across 15 countries.
www.forcepoint.com/Hogan-Lovells-Privacy-Guide

FORCEPOINT