INFORMATION COMPLIANCE

PRIVACY AND SECURITY

FIND OUT MORE ABOUT HOW YOU CAN SAFEGUARD YOUR ORGANIZATION'S DATA AND COMPLY WITH CHANGING LAWS, REGULATIONS AND OPERATIONAL REQUIREMENTS.

DON'T LEAVE THE DOOR OPEN

We are living in an information-rich, knowledge-driven world. With such value placed on data, it's hardly surprising that information risk has become a far-reaching problem.

The digital age has transformed attitudes to private, sensitive information. Today, we'll quite happily share sensitive data via our smartphones and other devices in ways that were unthinkable just 15 years ago. Rules and regulations around data privacy have become more complex and strenuous in an effort to keep up. As a result, there's mounting pressure on organizations to safeguard data and evolve information compliance.

34% of people are more likely to share basic personal information online than three years ago.*

MAINTAINING PRIVACY

Personal Identifiable Information (PII) is the main driver for privacy and security compliance. PII includes any information that identifies individuals – from employees to customers and even volunteers. Disclosing it – whether voluntarily or by accident – can have dire consequences for both the individual in question and your organization.

3 MINUTE READ

Records and information management (RIM) professionals have a role to play in maintaining privacy and security compliance. The ever-changing nature of data security threats means you can't afford to stand still. You need a comprehensive strategy that includes people, products, processes and technology.

Our RIM Risk Guide white paper gives a thorough grounding in using self-assessment to understand your compliance risk.

PRIVACY AND SECURITY CONTROLS

The correct privacy and security controls will help you comply with any laws, regulations and operational requirements.

Appropriate controls include:

1. **Data classification**
   Classify data according to its value and sensitivity. It's crucial to have a data classification system in place to fully understand the scope and significance of any data threats.

2. **Secure access**
   Who has access to your data? Is access restricted at all? If so, to what extent does security restrict data access? Make sure your policy covers information access.

3. **Online security**
   RIM policy should include online security protocols. These protocols cover all devices, data locations and data types. BYOD is commonplace, but allowing people to use their own devices may mean your business data or plans for new products may end up in hostile hands.

4. **Secure shredding**
   Inadequate disposal of physical documents poses a significant data threat. A secure shredding protocol protects against the theft or inadvertent disclosure of PII.

5. **Media and e-waste disposal**
   Sensitive information is also stored electronically. Establish a defensible, repeatable and documented process for the safe disposal of hard drives, mobile devices and other places where PII is stored.

6. **Data breach incident reporting**
   What would you do were a data breach to occur? Clearly define the processes used to respond to any data breach, and apply this framework across your organization.

Compliance is not only an organizational responsibility, but also a personal one. Make every employee aware of his or her role in maintaining privacy and security compliance.

THE AVERAGE TOTAL COST OF EACH DATA BREACH IS $3.79 MILLION.**

WHAT NEXT?

You can learn more about the role of RIM self-assessment in privacy and security compliance in our RIM Risk Guide white paper. Download the paper here, and read more in our Practical Guide to Information Governance.

* Research was undertaken for Iron Mountain by Opinion Matters. It questioned a total of 4,006 workers in mid-market companies (250-3,000 employees – 250-5,000 in North America) across the UK, France, Germany, The Netherlands, Belgium, Spain and North America.

** Source: 2016 Ponemon Cost of Data Breach Study - Global Report. Available at: http://www-03.ibm.com/security/data-breach/