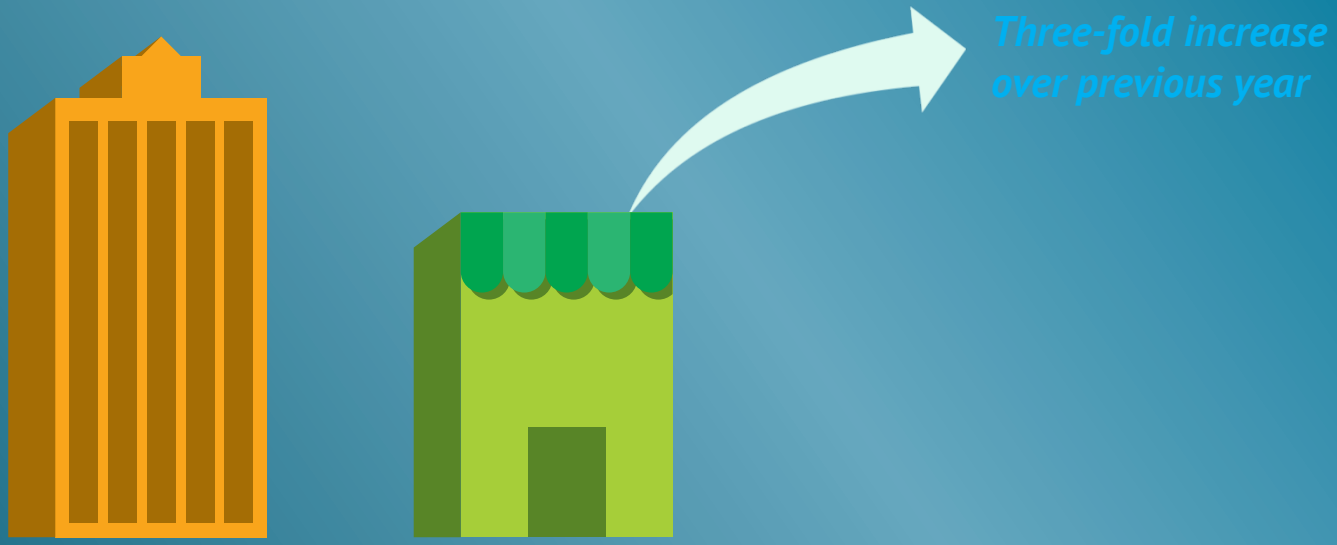
The need for an integrated security management platform

Fran Howarth
Senior analyst, security

Breach victims

"It's not if, but when and how often"



81%

Large organisations

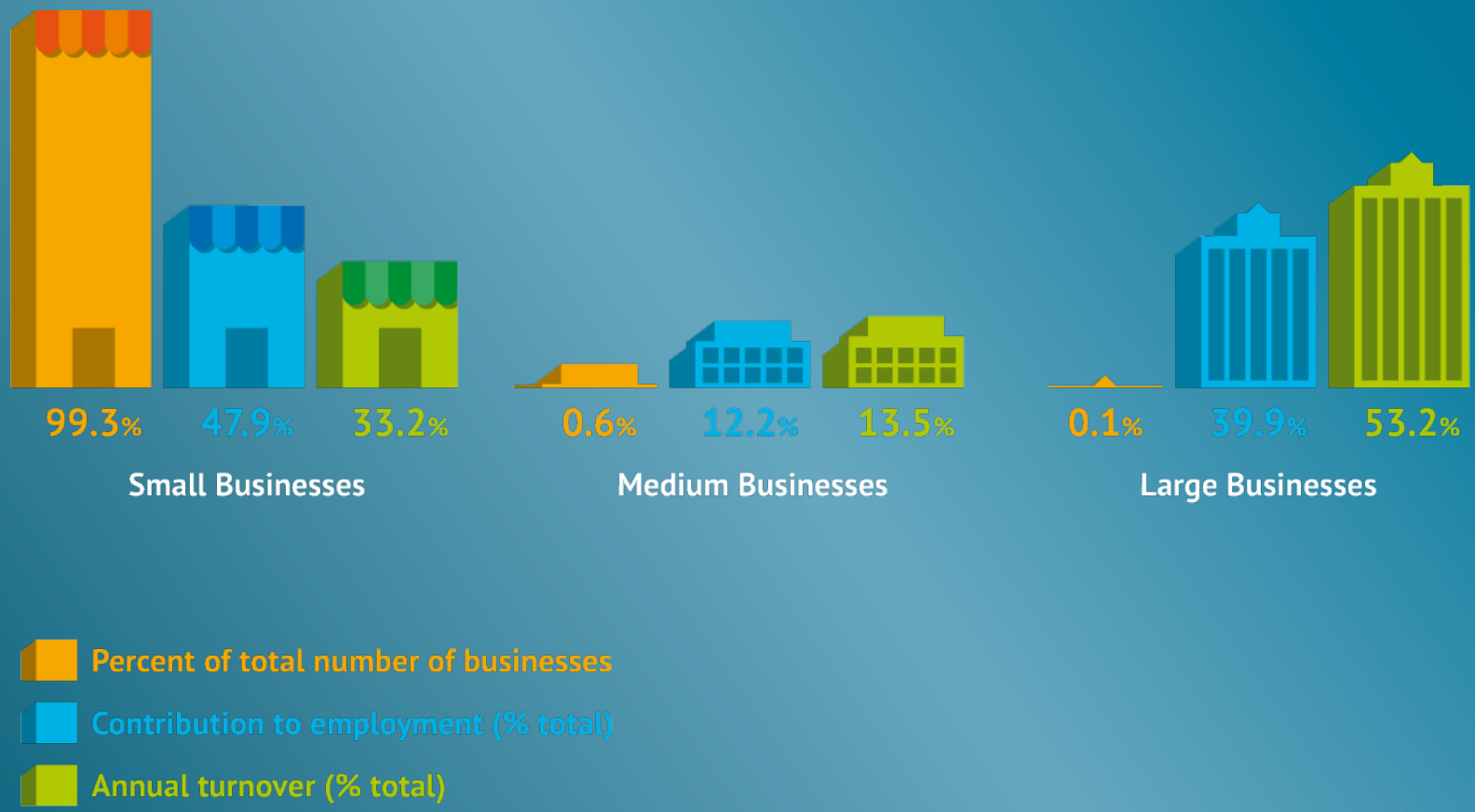
60%

Small and medium organisations

Source: PwC/Infosec Europe 2014, Symantec

Smaller firms in danger

Smaller firms vital for the economy



Source: UK Department for Business, Innovation & Skills

Challenges in threat detection for SMEs

Source: Ponemon Institute

A more proactive response

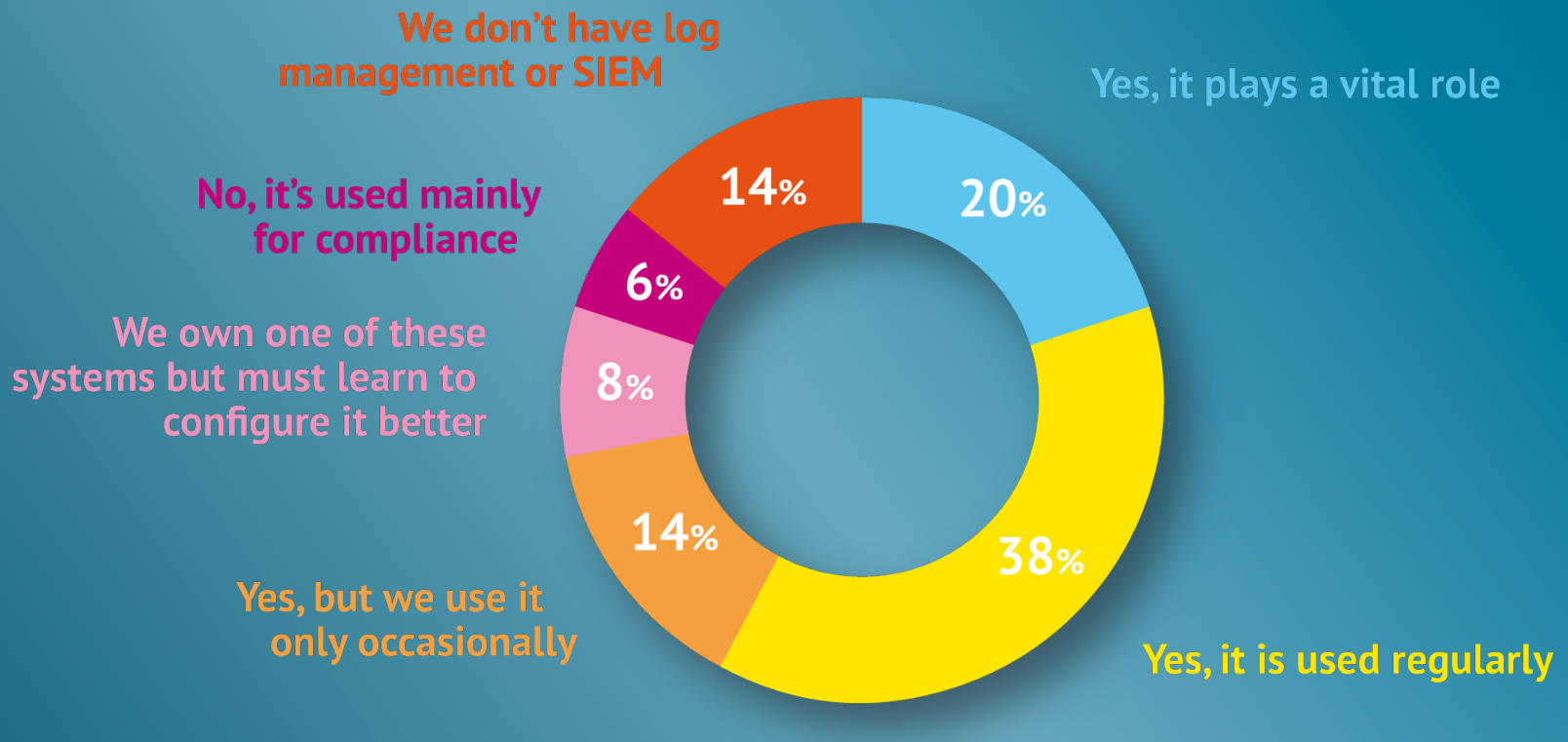
A unified security management platform:

- Asset discovery
- Vulnerability and threat management
- Threat identification and management
- Behavioural monitoring
- Security intelligence
- Centralised management

Asset discovery

Vulnerability and risk assessment

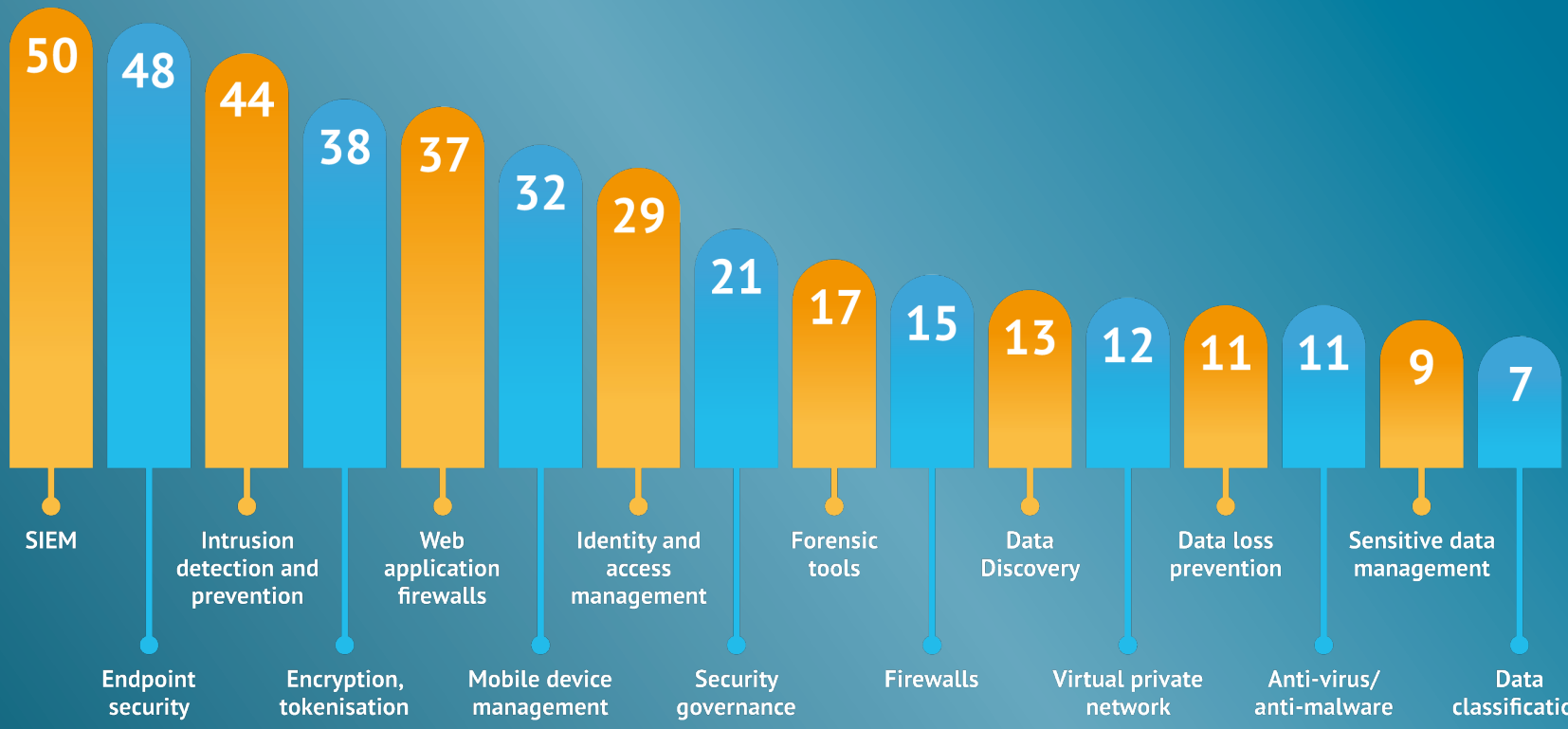
Threat identification: the role of threat intelligence



Source: InformationWeek

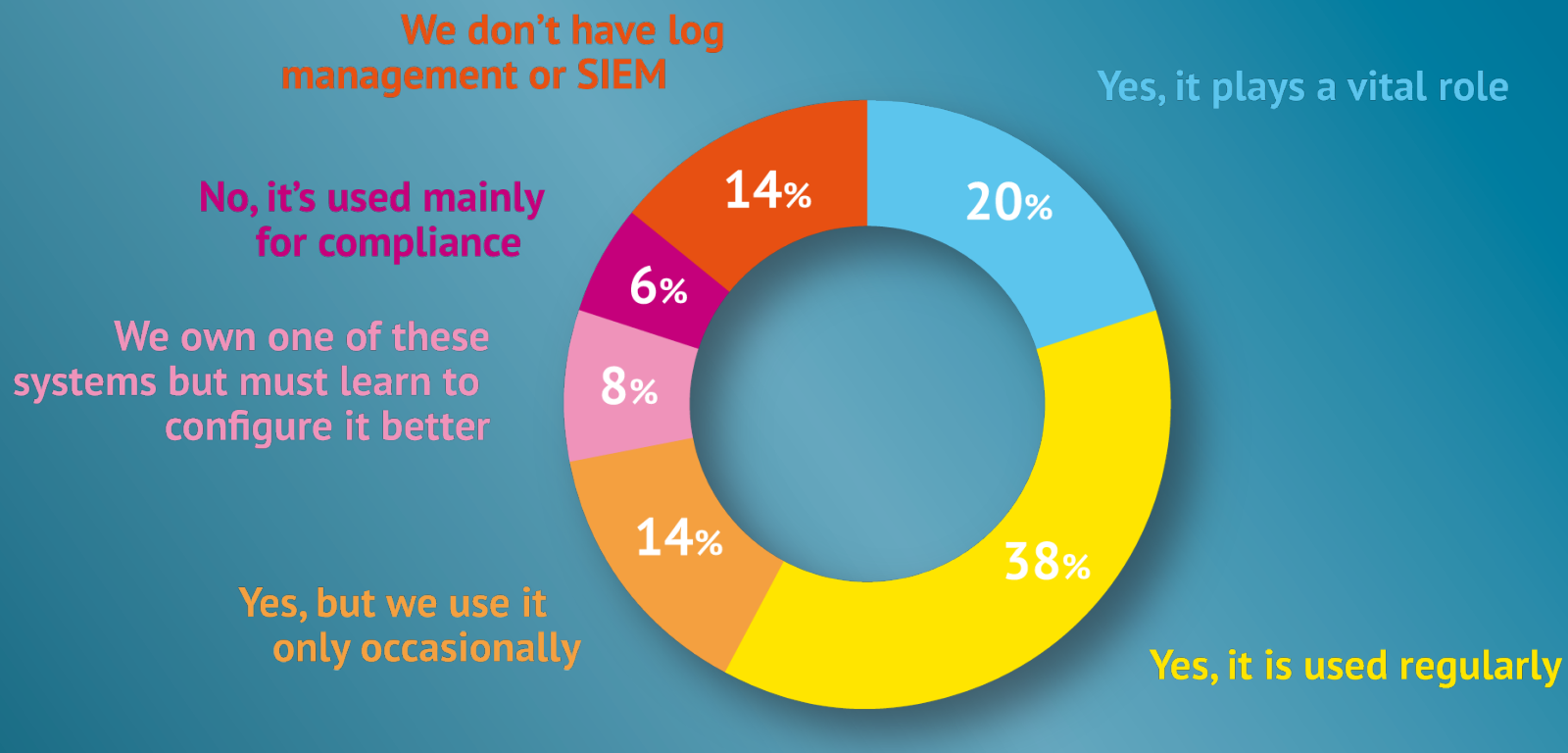
Behavioural monitoring

Technology investments in event of breach



Source: Ponemon Institute

Use of SIEM for security intelligence



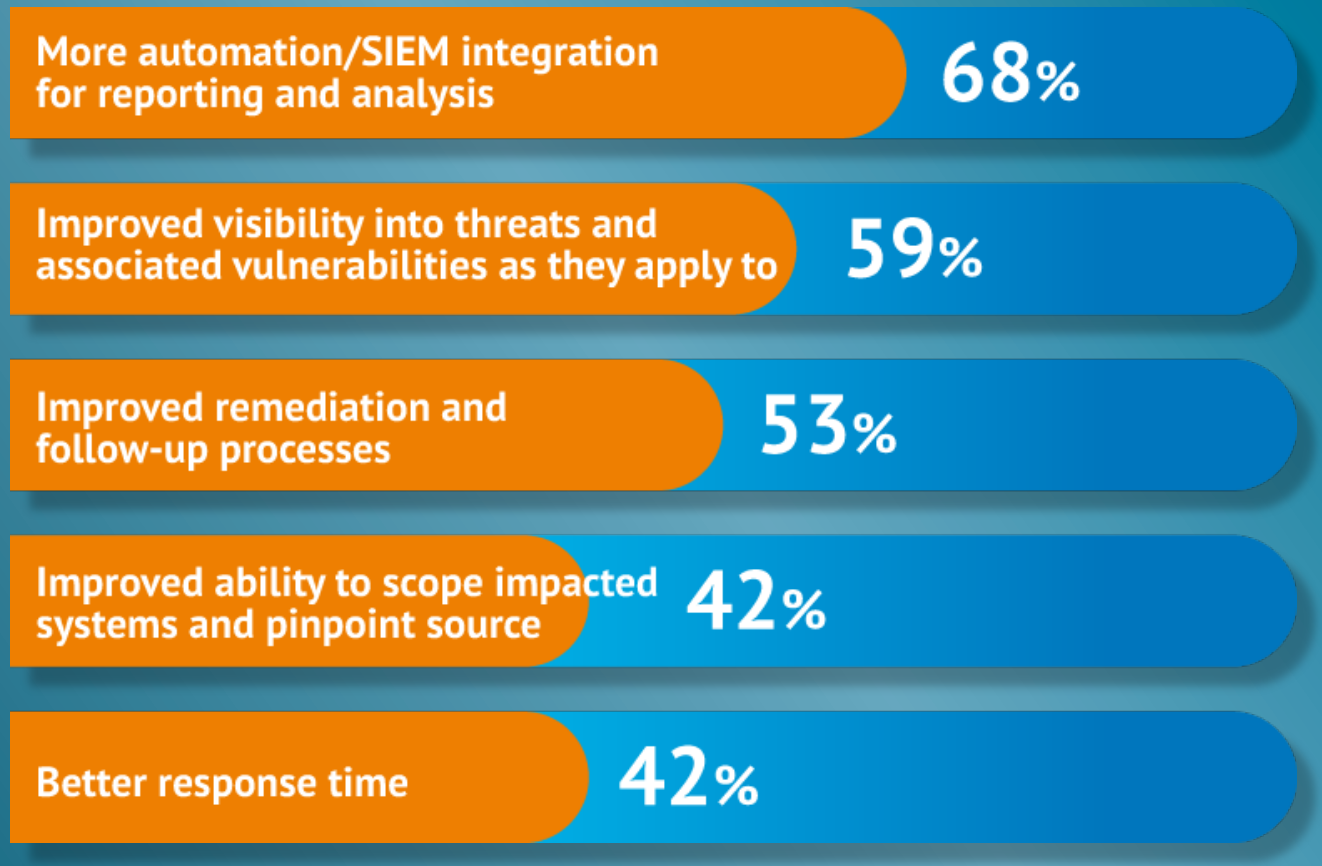
Source: InformationWeek

Recommendations

- Integrate tools into a single operating console or dashboard
- Maintain a continually updated software inventory
- Use continuous vulnerability monitoring
- Complete a hardware inventory
- Use network mapping
- Incorporate log aggregation and correlation
- Take threat intelligence feeds for threat identification and prioritisation

Source: SANS Institute

Expected improvements for incident response



Source: SANS Institute

Advantages of security management platforms

- Correlation of data from throughout network
- Anomaly detection
- Comprehensive visibility
- Advanced threat protection
- Risk prioritisation
- Alerting and monitoring
- Customise according to business needs
- Demonstrate adherence to policies and controls
- Protect sensitive data
- Limit exposure to breach disclosure
- Reduce risk to business partners and customers
- Reduce costs